Pakistan Journal of Life and Social Sciences
www.pjlss.edu.pk

https://doi.org/10.57239/PJLSS-2024-22.2.001168

RESEARCH ARTICLE

The Role of Government Secondary School Teachers in Applying Artificial Intelligence to Activate Risk Management and Achieve Cybersecurity from the Students' Point of View

Athir Husni Al Kouri [1*], Mohammad Alsa'di[2], Shireen Al_Qawasmeh[3], Morsi Mustafa Abu Salih[4], Rami Ali Sadi[5]

[1] The Islamic University of Minnesota, USA
[2] Ajloun National University, Jordan
[3] Palestine Polytechnic University (PPU), Palestine
[4] David Yallin College of Education, Sakhnin
[5] Al-Qasemi Academic College (R.A), Arrabe

ARTICLE INFO

Received: Oct 2, 2024

Accepted: Nov 15, 2024

Keywords

Artificial Intelligence

Risk Management

Cybersecurity

Government Secondary Schools

Teachers

Students

Kingdom of Bahrain

***Corresponding Author:**

athirkouri@gmail.com

ABSTRACT

The study aimed to identify the role of government secondary school teachers in applying artificial intelligence to activate risk management and achieve cybersecurity from the students' point of view. The study followed the descriptive survey method, and the study used a questionnaire consisting of (20) items to collect its data, and it consisted of two axes: artificial intelligence in the process Educational, and requirements for achieving cybersecurity, and their validity and reliability were verified. The study sample consisted of (131) male and female students who were selected randomly. The results of the study showed that the role of teachers in schools in applying artificial intelligence to activate risk management and achieve cybersecurity from the point of view of the study community was at a (medium) degree in all areas, where the arithmetic average was (3.07), and that the field of "artificial intelligence in the educational process" was at a degree (Medium), with a mean of (3.49), and that the field of "requirements to achieve cybersecurity" was at a degree of (medium), with a mean of (2.64). The researchers also recommended "adopting a risk management method to achieve cybersecurity while providing all the physical capabilities, tools and means that work." To constantly develop and update information and technology programs and applications.

INTRODUCTION

The world is witnessing widespread development in various fields and activities in light of the rapid changes, and its impact is clearly visible in educational institutions. The era in which we live is the era of the technological and cognitive revolution, which relies heavily on the Internet, information and communication technologies, and artificial intelligence, and personal and confidential information can be exposed to hacking and exploitation. It is exposed to criminal activities, its services are disrupted, and its property is destroyed. A sense of insecurity appears here. Hence, the importance of activating risk management, where risks are predicted before they occur, and precautionary and preventive measures are activated. Educational institutions must realize that their digital agenda should be based on a disciplined approach. To manage risks and enhance cybersecurity, which seeks to protect human and financial resources associated with communications and information technologies, and the goal is to limit the losses and damages that result if security risks and threats materialize in cyberspace.

Passmore (2016) pointed out that dealing with the field of modern communication and Internet technologies involves real challenges and risks, and here appears the task of risk management by confronting various risks resulting from the increasing uses of technology in educational institutions, including: risks related to the uses of new technologies, and risks resulting from the distribution of Data(Alsadi, et all 2024), risks resulting from the integration of technical work, the size of existing devices, equipment and technical tools, and risks resulting from a lack of awareness of behavior in certain situations. He also pointed out the impact of technical risks on the educational institution and on its internal and external environment, where risk management leaders can confront them when implementing projects. Huge technology.

There is no doubt that the security and protection of information, property and infrastructure and achieving the requirements of cybersecurity (confidentiality, integrity, availability) are among the most important issues in the current era. The success of any organization depends greatly and clearly on the information it possesses and the extent of its preservation. It must We keep in mind that this information and systems are exposed to risks from time to time; The reason for this is because it faces multiple types of information breaches, and we cannot ignore the criminal activities (unethical hackers) to which it is exposed, and they work to disrupt its services, destroy its property, and attempt unauthorized access. Unethical hacker attacks occur in... Different images from one side to another, from one place to another and from time to time; As it uses modern, renewed and advanced hacking tools, mechanisms and techniques all the time; This emphasizes the importance of achieving the goals of cybersecurity and its urgent necessity in the current era (Al-Shaya, 2019)

Previous Studies:

The following is a review of previous studies related to the subject of this study, in terms of their focus on the study's goal, methodology, and tools, and they were dealt with in chronological order from oldest to most recent.

Previous Studies Related to Artificial Intelligence:

The study by Al-Subhi and Al-Farani (2020) aimed for the Kingdom of Saudi Arabia to adopt modern technology such as artificial intelligence after studying education in light of the capabilities, requirements, and challenges, in addition to identifying the extent to which faculty members accept this technology and adopt it in the university educational process, so that the study concludes that there is a slight slowdown in Efforts to develop Saudi education, and the necessity of adopting artificial intelligence because it is the technology of the era.

Al-Muqiti's study (2021) came to identify the reality of employing artificial intelligence in the academic and administrative fields and its relationship to the quality of performance of Jordanian universities from the point of view of the faculty members consisting of (370) members. The results showed an average level of the degree of employing artificial intelligence, and also indicated that there were no differences. Among faculty members, it was attributed to the variable of gender, academic rank, and number of years of experience. On the contrary, it created differences due to the type of college in favor of scientific colleges. It also resulted in a statistically significant correlation between the degree of employing intelligence and the overall score for the quality of performance of Jordanian universities.

Previous Studies Related to Risk Management

The study by Sum & Saad (2017) aimed to identify and clarify the importance of risk management in the academic environment and to enhance knowledge and understanding of risks in the context of higher education. It also aimed to correct people's perceptions of risk management. The study population consisted of Malaysian public universities and the study sample was limited On the university environment (Universiti Islamic Sciences Malaysia), as it contributed to enhancing understanding in risk management, and highlighted that it is an effective management tool to help universities achieve their strategic goals, and the study recommends investigating how to include risk management processes in the basic management courses of the university, and developing a management framework. Risks that are appropriate to the university environment.

The study Yokoyama (2018) aimed to identify how the state of uncertainty and insecurity in the post-2008 period led to the reshaping of risk management in university systems. The study examines internal control in the contexts of the English university system and the State University of New York (SUNY) system. The concept of "risk" was used by exploring the theses of the "risk society". The paper argues that the uncertainty, anxiety and mistrust following the 2008 financial crisis did not reshape risk management mechanisms in England and the SUNY system. The adaptive responses of these university systems to the crisis were immediate responses to financial shortfalls, rather than reforms of internal control mechanisms. This suggests that an uncertain environment may push universities into a reflexive mode; However, fundamental structural changes are not necessary.

The study of Zaqzouq and Al-Sarihi (2019) aimed to Identifying the competencies of leaders and their effective role in risk management in institutions, as he pointed out that risk leaders possess a complex set of competencies to enable their organizations to recover from crises. They possess a complex set of competencies such as detecting signals quickly and intelligently and controlling and containing damage. To achieve this, there must be Professional competencies. At the same time, it is necessary not to be preoccupied with details, the ability to analyze and read variables in the work environment, and the ability to set priorities. The study, through analyzing the content of relevant studies in a documentary study of intellectual production, reached important leadership competencies and skills and demonstrated them in the study.

Al-Abdul Rahman's study (2021) aimed to identify the possibility of applying risk management in Jordanian universities among academic and administrative leaders. The study relied on the partial descriptive survey method, and the study sample consisted of (331) academic and administrative leaders from the leaders of Jordanian universities. The results concluded that the possibility of applying Risk management in Jordanian universities among academic and administrative leaders was (moderate), and the results showed that there were no statistically significant differences at the level of significance (a = 0.05) between the average estimates of the sample members due to the effect of gender in all fields except the field of risk management policy implementation. Differences in favor of females.

Previous Studies Related to Cybersecurity:

Al-Muntashari's study (2020) aimed to find out the role of school leadership in enhancing cybersecurity in government schools for girls in Jeddah from the teachers' point of view. The analytical approach was used, and the study sample consisted of (420) teachers in government schools in Jeddah. The results of the study showed that the role School leadership in enhancing cybersecurity among teachers came to a (low) degree, and one of the most important proposals of the study is protecting the physical environment of the Internet.

Al-Shehri's study (2021) aimed to identify the role of university administration in enhancing awareness of cybersecurity among students of the College of Education at Imam Muhammad bin Saud Islamic University. The study relied on the descriptive survey method, and the study sample consisted of (188) male and female students. The results concluded that The students' knowledge of cybersecurity was (medium), and the university administration's exercise of its role in enhancing awareness of cybersecurity among students was (medium).

Al-Manea's study (2022) aimed to identify the reality of achieving cybersecurity in Saudi universities in light of Vision 2030. The descriptive analytical approach was used, and the study population consisted of all technical employees of three Saudi universities, and their number reached (468) employees, and a random sample of (468) employees was chosen. 210) employees, and the results of the study showed that the reality of achieving cybersecurity in Saudi universities in light of Vision 2030 was at a (moderate) degree. The results of the study also showed that there were obstacles to achieving cybersecurity, which were at a (significant) degree, and among the most important obstacles is the low level of experience among employees, One of the most important proposals is educating employees about the dangers of using personal devices at the university.

Previous studies varied in terms of their objectives and the variables they addressed, and this study was distinguished from other previous studies by being the first study within the researchers' knowledge that addressed the role of faculty members in public universities in applying artificial intelligence to activate risk management and achieve cybersecurity from the students' point of view, in addition to its distinction. Unlike other previous studies in the areas of the study tool and its sample, and from here it can be said that there is an urgent need to conduct this study, and the previous studies have benefited from enriching the theoretical literature, developing the study tool, the statistical methods used, and discussing and comparing the results.

Study Problem and Questions:

Given the roles that educational institutions play in the educational system, as they are the link between all elements of the educational process, including administrators, faculty, curricula, and students, they only require the educational institution (universities) to organize matters and plan that depends on strategies and methods that develop and encourage the use of technology and keep up with developments, which It will directly affect students' performance, thus achieving educational goals efficiently and effectively.

It has recently been observed that countries of the world are suffering from the danger of cyber attacks, as the Hashemite Kingdom of Jordan was subjected during the year (2021) to (897) cyber attacks documented by the National Center for Cyber Security, representing (27%) of the cyber attacks, that is, about (240). The attacks were of a complex type, which negatively affects the performance of the teaching staff and may affect the nature of the conduct of educational processes and their outcomes (Government: Jordan was subjected to 897 cyber attacks, 2022). Both the Al-Manea study (2022) and the Al-Muntashari study (2020) confirmed) on the importance of educating workers about achieving and activating cybersecurity.

Based on the above, the problem of the study is to try to know the role of faculty members in public universities in applying artificial intelligence to activate risk management and achieve cybersecurity, by answering the following questions:

What is the role of university faculty members in applying artificial intelligence to activate risk management and achieve cybersecurity from the students' point of view?

Are there statistically significant differences at the significance level (a=0.05) between the averages of the responses of the study sample members about the role of faculty members in public universities in applying artificial intelligence to activate risk management and achieve cybersecurity from the students' point of view due to differences in variables: (gender, years' experience)?

Objectives of the Study:

This study seeks to identify the role of faculty members at public universities in applying artificial intelligence to activate risk management and achieve cybersecurity, and to reveal whether there are statistically significant differences between the average ratings of the members of the study sample for the role of faculty members at public universities in applying artificial intelligence to activate risk management and achieve Cybersecurity from the students' point of view is due to the gender variable.

The Importance of Studying:

Given the importance of the educational institution's effective role in activating and developing the educational process, the importance of the current study comes from its theoretical importance and practical importance as follows:

-Theoretical importance: represented by the lack of Jordanian studies and a new study community, as no study of this kind has been conducted - to the knowledge of the researchers - in Bahrain that addresses the role of teachers in schools by applying artificial intelligence to activate risk management and achieve cybersecurity from the students' point of view. It is also possible that the importance of this study is highlighted by its targeting of the focus of the educational system, which is maintaining a safe atmosphere away from the risks that may occur in educational institutions.

-Practical importance: The results of this study can benefit educational institutions by learning about ways and methods of activating risk management to achieve cybersecurity, by employing the results, recommendations and suggestions reached by this study, alerting to deficiencies in performance and working to fill these gaps. It is hoped it will also benefit officials in the Ministry of Education to work to put in place appropriate amendments and decisions in an appropriate regulatory environment that encourages, facilitates and activates the role of risk management to achieve cybersecurity.

Terminological and Procedural Definitions:

The study included some terms that were defined terminologically and procedurally as follows:

Artificial Intelligence: "It is the science that seeks to develop computer systems that operate with high efficiency, that is, it is the ability of a machine to imitate and simulate the motor and mental processes of a person, and the way his mind works in thinking, deducing, responding, and benefiting from previous experiences and intelligent reactions; it is emulation." The human mind and playing its role" (Qatami, 2018, 14; Jam et al., 2012), and the researchers define artificial intelligence procedurally as: that philosophical aspect of the relatively modern computer, embodied in a group of smart technological applications that simulate human intelligence and a technology that humans use to perform their tasks with high precision and flexibility.

Cybersecurity: "A set of technical, administrative, and organizational means, the achievement of which leads to preventing misuse of the information network, preserving it, and ensuring the continuity of its work" (Atif and Qasim, 2019, 12; Hussein et al., 2024), and is defined procedurally as: preventing and protecting confidential and sensitive information whose purpose is to destroy or destroy it. Grab it.

Risk Management: "Activities and policies related to reaching specific means of controlling risk or reducing the size of the losses that result from that and the resulting reduction in the degree of risk from these activities, provided that this is accompanied by a reduction in the cost necessary to implement such policies and activities." (Al-Wadi and Al-Zoubi, 2011, 14), and is defined procedurally as: processes by which risks are measured and evaluated and strategies and plans are developed to manage them so that their negative effects are reduced.

Study Limitations:

This study was limited to a sample of (131) government secondary school students in the Kingdom of Bahrain, for the year 2023/2024, and its limitations are determined by the level of validity and reliability of the tool and the objectivity of the sample members' response to the tool's items.

METHOD AND PROCEDURES:

This part included a description of the study methodology, the study population and sample, the study tool, the procedures necessary to verify the validity and reliability of the study tool, and the statistical procedures and methods that were used in analyzing the data.

Study Approach:

A descriptive survey approach was used to identify the role of teachers in secondary schools in applying artificial intelligence to activate risk management and achieve cybersecurity from the perspective of students in the Kingdom of Bahrain.

Study Sample and Population:

The study sample was selected randomly from the study population. The study population included (131) male and female students. An electronic questionnaire was distributed to the study sample members. Table (1) shows the frequencies and percentages of the study sample members according to their variables.

Table (1): Distribution of study sample members according to its variables

Variable	Level/category	The Number	Percentage%
Gender	Male	54	41.2
	Female	77	58.8
	Total	131	100.0

Table (1) shows that the percentage of females is the highest (58.8%), while the percentage of males is (41.2%).

Study Tool:

For the purposes of developing the study tool, reference was made to theoretical literature and previous relevant studies.

Validity of the Study Tool:

To verify the validity of the questionnaire's content, it was presented in its original form to a group of arbitrators specialized in educational administration and cybersecurity in Jordanian and Bahraini universities. They were asked to judge the questionnaire in terms of its suitability to reveal the role of teachers in schools by applying artificial intelligence to activate risk management and achieve cybersecurity from the point of view of Students, the clarity of the paragraphs, and any comments and modifications they deem appropriate. The arbitrators indicated that the scale is suitable for revealing and identifying the role of teachers in schools by applying artificial intelligence to activate risk management and achieving cybersecurity from the students' point of view. Minor comments and modifications were made to the questionnaire, and it was Taking it.

Stability of the Study Tool:

To verify the stability of the mental rotation test (stability stability), the test-retest method was used by applying it to a survey sample from outside the study sample, consisting of (5) students, and the application was repeated on the same sample after a time interval of two weeks from application. First, using the Pearson correlation coefficient, the reliability of the test was verified (reliability stability), which reached (0.85), and the Cronbach alpha equation was used to verify the reliability (internal consistency) of the test, which reached (0.87).

Study Procedures:

The problem of the study was identified, a plan was drawn up, the study tool was prepared, its validity and reliability were verified, then approval was obtained to implement the study in coordination with the concerned authorities, then the questionnaires were distributed to all members of the study sample, then they were collected after a period of time, unpacked, and entered into the computer using the (SPSS) program. To treat them statistically, conduct appropriate statistical analyses, then extract and interpret the results, and provide appropriate recommendations in light of the results.

Statistical Processing:

In order to calculate the total score for the tool, five alternatives were developed. The respondent chooses one of these alternatives that expresses his opinion. Grades (5, 4, 3, 2, 1) were given for the five alternatives, respectively, for the paragraphs. A score of (5) was given for the alternative, which is very high. A score of (4) was given to the alternative - high, a score of (3) was given to the alternative - moderate, a score of (2) was given to the alternative - low, and a score of (1) was given to the alternative - very little. A triple gradation was also adopted for the purposes of interpreting the results, which is (to a large degree, moderate, Low), and to judge the level of arithmetic averages for items, fields, and the tool, the statistical standard was adopted using the following equation:

Category range = (highest value - lowest value) divided by the number of options

Class length= 5-1= 4 ÷3= 1.33

Thus, the criterion for judgment becomes as follows:

Table (2): The statistical standard for determining the role of teachers in schools by applying artificial intelligence to activate risk management and achieve cybersecurity from the students' point of view

SMA	Average Score
From 1.00 -2.33	Low
From 2.34 - 3.67	Medium
From 3.68 -5.00	Large

STUDY RESULTS AND DISCUSSION:

This part included a presentation of the results reached by this study through the sample members' answers to the study's questions, as follows:

Results Related to the Answer to the first Question: What is the role of teachers in schools in applying artificial intelligence to activate risk management and achieve cybersecurity from the students' point of view?

To answer this question, the arithmetic means, standard deviations, ranks, and item scores were calculated for each item separately, and then the total score for each area of the questionnaire, and Table (3) shows the results related to that.

Table (3): Arithmetic means and standard deviations for the role of teachers in schools by applying artificial intelligence to activate risk management and achieve cybersecurity from the students' point of view.

Ranking	The Field	The Field	SMA	Standard Deviation	Class
1	First Field	Artificial Intelligence in the Educational Process	3.49	.664	Medium

2	Second Field	Requirements for Achieving Cybersecurity	2.64	.948	Medium
		Total Marks	3.07	.727	Medium

Table (3) shows that “The first field: “Artificial intelligence in the educational process” came in first place with an arithmetic mean (3.49) and a standard deviation of (.660) with a score of (medium), and “The first field: Requirements for achieving cybersecurity” came in second place. With an arithmetic mean of (2.64) and a standard deviation of (.940) and a (medium) degree, the arithmetic mean for the role of teachers in schools in applying artificial intelligence to activate risk management and achieving cybersecurity from the point of view of students as a whole was (3.07) and a standard deviation of (.720) and a (medium) degree.(.

This may be due to the school’s weak possession of high-level systems and plans to activate risk management to achieve cybersecurity. This may also be due to the lack of a secure networking system for exchanging administrative information and applying administrative procedures within the school’s administrative information systems. These results are consistent with the results of Al-Abdul Rahman’s study (2021).) which showed the possibility of applying risk management in Jordanian universities among academic and administrative leaders.

Arithmetic means and standard deviations were also calculated for the estimates of the study sample members on each of the paragraphs of each area of the role of faculty members at Irbid National School in activating risk management to achieve cybersecurity. The following is a presentation of that:

The First Area: Artificial Intelligence in the Educational Process

The arithmetic means and standard deviations of the study sample's estimates on the items in the field of artificial intelligence in the educational process were calculated, and were as shown in Table (4).

Table (4): Arithmetic means in descending order and standard deviations related to the field of artificial intelligence in the educational process

Number Paragraph	Section	Average Arithmetic	deviation Standard	rate	Class
	Programs supported by artificial intelligence technology help students learn skills	4.60	524.	1	Large
	It helps students to break free from one-style education	4.34	609.	4	Large
	Reduces the stress of trial and error in learning	4.32	630.	5	Large
	The teacher has become a facilitator and guide of the educational process only	4.40	627.	2	Large
	It helps students make appropriate educational decisions	4.36	775.	3	Large
	It provides a learning style for each student according to his inclinations, trends, and needs	2.39	1.476	10	Medium
	More accurate in determining the student's level compared to traditional systems	2.66	1.524	7	Medium

	Students can learn anytime and anywhere in the world	2.59	1.529	8	Medium
	It forces the student to think about how to use information rather than just looking for it	2.74	1.498	6	Medium
	It reduces the number of hours of learning various courses.	2.50	1.515	9	Medium
	Artificial intelligence in the educational process	3.49	.664		Medium

It is noted from Table (4) that the arithmetic means for the domain items ranged between (4.60) and (2.39), with a degree of (large to moderate). Paragraph (1) stated: "Programs supported by artificial intelligence technology help students learn basic skills." In first place, with a mean of (4.60), a standard deviation of (0.52), and a degree of (large), while paragraph (6) came, which stated, "Providing a learning style for each student according to his inclinations, trends, and needs." In the last order, (2.39), standard deviation (1.476) and (medium) degree.

This may be due to the presence of some programs supported by artificial intelligence technology and the great advantages that benefit students in learning basic skills and modern and technological techniques.

The Second Area: Requirements for Achieving Cybersecurity

Arithmetic means and standard deviations were calculated for the items in the field of requirements for achieving cybersecurity, and the results were as in Table (5).

Table (5): Descending arithmetic means and standard deviations related to the domain of cybersecurity requirements

Number Paragraph	Section	Average Arithmetic	deviation Standard	rate	Class
11	Providing financial allocations to achieve cybersecurity.	2.66	1.486	5	Medium
12	Constantly developing and updating information and technology programs and applications.	2.23	1.455	9	Medium
13	Awareness of the dangers of using personal devices such as a mobile phone to store or transmit confidential school information.	2.32	1.458	8	Medium
14	It holds periodic meetings for cybersecurity specialists to inform them of the latest developments in this field.	1.41	0.991	10	Low
15	Distributing awareness brochures on forms of cybercrime.	2.56	1.479	7	Medium
16	Warning not to disclose personal data in cyberspace.	3.37	1.561	1	Medium
17	Allocate counseling sessions for those exposed to cyber risks.	2.98	1.509	4	Medium
18	Instructing all school computer users not to leave devices open without use.	3.06	1.538	3	Medium

19	Involving faculty members in developing practical programs to introduce cybersecurity and mechanisms for enhancing it.	2.61	1.481	6	Medium
20	Applying administrative procedures to achieve cybersecurity within the school's administrative information systems.	3.23	1.444	2	Medium
	Requirements for achieving cybersecurity	2.64	.9480		Medium

It is noted from Table (5) that the arithmetic averages for the domain items ranged between (3.37) and (2.38), with a degree of (medium to low). Paragraph (16) stipulates "warning against disclosing personal data in cyberspace." In the first ranking, with an arithmetic mean of (3.37), with a standard deviation of (1.561), and with a degree of (medium), while paragraph (14) which stipulates: "Periodic meetings are held for cybersecurity specialists to inform them of the latest developments in this field." In the last ranking, with an arithmetic mean (1.41) with a standard deviation of (0.991) and a degree of (medium).

This may be due to the weakness of information protection policies and their failure to keep pace with the prevailing changes in the field of school security hacks and threats. These results are consistent with the results of Al-Manea's study (2022), which showed that the reality of achieving cybersecurity in Saudi universities in light of Vision 2030 was at a (moderate) degree.

Second: Results Related to the Second Question: Are there statistically significant differences at the significance level (α = 0.05) in responses regarding the role of teachers in schools in applying artificial intelligence to activate risk management and achieve cybersecurity from the students' point of view due to the variable (gender)?

To answer this question, the arithmetic means and standard deviations of the sample members' estimates were calculated on the axes of the role of teachers in schools by applying artificial intelligence to activate risk management and achieve cybersecurity from the students' point of view due to the variable gender, as they were as shown in Table (6).

Table (6): The results of the t-test for the significance of the differences between the average responses of the study sample members due to the gender variable

	Gender	**Number**	**SMA**	**Standard Deviation**	**T-test**	**Level of statistical significance**
Variable	Male	54	3.00	.745	1.799	.182
	Feminine	77	3.11	.715		

Statistically significant at the significance level (a=0.05)

It is noted from Table (7) that there are no statistically significant differences between the averages of the responses of sample members to study the role of teachers in schools by applying artificial intelligence to activate risk management and achieve cybersecurity from the students' point of view due to the gender variable, where the value of (level of statistical significance) was (0.182), which is A value that is not statistically significant at the significance level (0.05) between males and females.

Recommendations:

In light of the results of the study, the researchers recommend the following:

- Adopting a risk management method to achieve cybersecurity while providing all the material capabilities, tools and means that work to constantly develop and update information and technology programs and applications, and involving faculty members in developing practical programs to introduce cybersecurity and mechanisms for enhancing it.

- Applying administrative procedures to achieve cybersecurity within the school's administrative information systems, and warning against disclosing personal data in cyberspace.

- Holding training courses to learn about the latest developments in activating risk management, and allocating guidance sessions for those exposed to cyber risks.

SOURCES AND REFERENCES

Al Shehri, Maryam (2021). The role of the university administration in enhancing awareness of cybersecurity among students of the College of Education at Imam Muhammad bin Saud Islamic University, *Journal of Humanities and Administrative Sciences*, 25, 83-104.

Al-Abdul Rahman, Asmaa (2021). The possibility of applying risk management in Jordanian universities from the point of view of academic and administrative leaders, *Journal of the Islamic University for Educational and Psychological Studies*, 29 (1), 420-443.

Al-Manea, Al-Jawhara (2022). Requirements for achieving cybersecurity in Saudi universities in light of Vision 2030, *Scientific Journal of the Faculty of Education*, Assiut University, 38 (1), 156-194.

Al-Montashari, Fatima (2020). The role of school leadership in enhancing cybersecurity in government schools for girls in Jeddah from the teachers' point of view, *Arab Journal of Educational and Psychological Sciences*, (17), 457-484.

Al-Muqiti, Sajoud Ahmed. (2021). *The reality of employing artificial intelligence and its relationship to the quality of performance of Jordanian universities from the point of view of faculty members.* Middle East University, Faculty of Educational Sciences, Master's Thesis, Amman, Jordan.

Alsadi, M. M., Momani, K. S. A., Daradkah, A. M., Alomari, M. A., & Awais, B. E. (2024). The Impact of E-Learning on Learnlng Out Comes at the Jordanian Universities. Revista de Gestão Social e Ambiental, 18(5), 1-17. https://doi.org/10.24857/rgsa.v18n5-141

Al-Shaya, Khaled (2019). *Cybersecurity: Its Concept, Characteristics, and Policies*, Saudi Arabia: Al Dar Al Alamiah.

Al-Sobhi, Nour Abdel Aziz, and Al-Farani, Lina Ahmed. (2020). Artificial intelligence in higher education in the Kingdom of Saudi Arabia. *Arab Journal of Educational and Psychological Sciences*, College of Postgraduate Educational Studies, King Abdulaziz University, 4 (17).

Al-Wadi, Mahmoud and Al-Zoubi, Ali (2011). *Total Quality Management requirements as a tool for achieving competitive advantage in Jordanian universities* - an analytical study, a research paper presented to the Zarqa University Regular Conference, 15-17, March 2011.

Atef, Maryam and Qasim, Ayman (2019). *Cybersecurity, Saudi Arabia*: Jarir Bookstore.

Government: Jordan was subjected to 897 cyber attacks last year (2022, 2, 20). Kingdom, source: https://www.almamlakatv.com/news./

Hussein, M. M., Al-kawaz, U., Alwasiti, E. A., & Mossa, H. A. (2024). Evaluation of Seminal Plasma Chitotriosidase-1 Levels in A Samples of Iraqi Oligoasthenoteratozoospermic Infertile Men with & Without Varicocele. *Pakistan Journal of Life and Social Sciences*, *22*(1).

Jam, F. A., Haq, I. U., & Fatima, T. (2012). Phychological contract and job outcomes: Mediating role of affective commitment. *Journal of Educational and Social Research*, *2*(4), 79-79.

Passmore, E. (2016). Brave New World. In Migrating Large-Scale Services to the Cloud. *A press, Berkeley*, CA, (pp.7-31).

Qatami, Samir. (2018). Artificial intelligence and its impact on humanity. *Journal of Ideas towards a Civic Culture*, (357), 13-40.

Sum, M. & Saad, M. (2017, December, 5-6). *Risk Management in Universities*, Paper Presented at 3rd International Conference on Qalb Guided Leadership in Education Institutions International cater, Kept, Nilai Negeri Sembilan Malaysia.

Yokoyama, K. (2018). The Risk of Risk Management in the Universities: Anew Way to Understand Quality in University Management, *Journal Articles, Reports-Research*, (55), 16.

Zaqzouq, Hazem Mustafa and Al-Sarihi, Hassan bin Awad (2019). Identifying the competencies of leaders and their effective role in risk management in institutions, *Journal of Information Studies*, (23), 115-131.