Journal of Arabian Peninsula Centre
for Educational and Humanity Researches
Volume (3), Issue (22): 30 Sep: 2024
p: 51- 70
Copyright License

ISSN: 2707-742X

مجلة مركـــز جـــــزيرة العـــــــرب
للبحوث التـــربـــوية والإنسانية
المجلد (3)، العدد (22): 30 سبتمبر 2024م
ص: 51- 70
تاريخ الاستلام: 2024/7/15 القبول: 2024/09/16

The impact of information security systems on organizational learning capabilities in educational institutions in Arabic Countries[1]

Dr. Elham Ali "Sid Ahmed" Abdullah

Assistant Professor||Department of Information and Computer Systems|| Applied college|| Najran university

Email: elhamnile@gmail.com || Mobile: 00966532072326|| ORCID: https://orcid.org/0009-0001-2482-7219

ABSTRACT: The study aimed to analyze the impact of information security systems on organizational learning capabilities, such as knowledge sharing and organizational commitment, in educational institutions in Arab countries. The researcher employed a descriptive-analytical methodology, reviewing dozens of reference studies. The study consisted of an introduction and three main sections: (1) analyzing the impact of information security systems on organizational learning capabilities in educational institutions in Arab countries, (2) evaluating how educational institutions measure their organizational capabilities based on information security systems, and (3) identifying the challenges that educational institutions face in effectively implementing information security systems. The study revealed that information security involves physical, environmental, and cyber measures, which are essential for institutional success. It also found that Arab universities face various challenges, including cyber threats (such as phishing and malware), complex information systems management, a lack of cybersecurity skills and awareness, insufficient investment in cybersecurity, and the rapid pace of technological changes. Based on the findings, the researcher proposed a framework for enhancing information systems, which includes a vision, mission, values, strategic goals, and an operational plan to develop national expertise in cybersecurity and ensure robust data protection mechanisms. The researcher also recommended strengthening partnerships with international organizations, allocating the necessary budgets to update security systems, and providing continuous cybersecurity training. Future studies were suggested to explore the impact of artificial intelligence technologies on information security, the role of collaboration between educational institutions and security agencies, and the effectiveness of staff training on information security systems.

Keywords: information security, organizational learning capabilities, educational institutions

تأثير أنظمة أمن المعلومات على قدرات التعلم التنظيمي في المؤسسات التعليمية في الدول العربية [2]

د. إلهام على "سيد أحمد" عبد الله

أستاذ مساعد|| قسم نظم المعلومات والحاسب|| الكلية التطبيقية|| جامعة نجران

الهاتف/ 00966532072326|| الإيميل/ elhamnile@gmail.com|| أوركيد: https://orcid.org/0009-0001-2482-7219

المستخلص: هدفت الدراسة إلى تحليل تأثير نظم أمن المعلومات على قدرات التعلم التنظيمي مثل تبادل المعرفة والالتزام التنظيمي في المؤسسات التعليمية في الدول العربية، اعتمدت الباحثة المنهج الوصفي التحليلي لعشرات الدراسات المرجعية، وتكونت الدراسة من مقدمة

[1]- APA Citation Documentation: Abdullah, E. A. "S A". (2024). The impact of information security systems on organizational learning capabilities in educational institutions in Arabic Countries. ***Journal of the Arabian Peninsula Center for Educational and Humanitarian Research, 3***(22), 51-70. https://doi.org/10.56793/pcra2213223

2-**توثيق الاقتباس (APA)**: عبد الله، إلهام علي "سيدأحمد". (2024). تأثير أنظمة أمن المعلومات على قدرات التعلم التنظيمي في المؤسسات التعليمية في الدول العربية، ***مجلة مركز جزيرة العرب للبحوث التربوية والإنسانية، 3***(22)، 51- 70. https://doi. org/10. 56793/pcra2213223 .

وثلاثة مباحث رئيسة: (1) تحليل تأثير نظم أمن المعلومات على قدرات التعلم التنظيمي في المؤسسات التعليمية في الدول العربية، (2) تقييم كيفية قياس المؤسسات التعليمية لقدراتها التنظيمية بناءً على نظم أمن المعلومات، (3) تحديد التحديات التي تواجه المؤسسات التعليمية في تنفيذ نظم أمان المعلومات بشكل فعال، وكشفت نتائج الدراسة أن أمن المعلومات يتضمن تدابير أمنية مادية وبيئية وفضائية، وهو أمر أساسي لنجاح المؤسسة، وأن الجامعات العربية تواجه تحديات متنوعة من التهديدات السيبرانية (مثل التصيد والبرمجيات الخبيثة)، إدارة نظم المعلومات المعقدة، نقص المهارات والوعي في مجال الأمن السيبراني، عدم كفاية الاستثمار في الأمن السيبراني، وسرعة التغيرات التكنولوجية. بناء على النتائج قدمت الباحثة تصورا لتفعيل أنظمة المعلومات تضمن (رؤية، رسالة، قيم، أهداف استراتيجية، خطة تشغيلية) لتطوير الخبرات الوطنية في مجال الأمن السيبراني وضمان آليات قوية لحماية البيانات. كما أوصت بتعزيز الشراكات مع المؤسسات الدولية، تخصيص الميزانيات اللازمة لتحديث نظم الأمان، والتدريب المستمر في الأمن السيبراني. كما اقترحت دراسات مستقبلية حول تأثير تقنيات الذكاء الاصطناعي على أمان المعلومات ودور التعاون بين المؤسسات التعليمية والجهات الأمنية وفعالية تدريب الموظفين على نظم أمن المعلومات.

الكلمات المفتاحية: أمن المعلومات، قدرات التعلم التنظيمي، المؤسسات التعليمية

1-Introduction.

The current era has witnessed an immense information explosion, leading institutions to face increasingly complex challenges amid constant environmental changes. According to Filali and Shlil (2018), institutions are subjected to a variety of threats, including natural disasters, human errors or deliberate attacks such as malware and cyber hacking. These institutions also face technical threats arising from security vulnerabilities, necessitating a comprehensive enhancement of information security through various forms of protection, including software, physical and legal measures.

In Saudi Arabia, a study by Al-Taimani (2021) highlighted the growing threats and frequent cyberattacks at all levels from individuals to institutions, ministries, and companies. The study noted that governments and companies are gradually recognizing the dangers of cybercrimes and the importance of information security for the economic and political stability of the country. The anonymity provided by the internet makes it a haven for cybercriminals, who benefit from high rewards, low risks of detection and difficulties in proving cybercrimes.

A study by Andijani and Filmban (2021) demonstrated the importance of enhancing cyber security awareness in Saudi Arabia. The study, which reviewed data from 2015 to 2020, emphasized the significance of social, environmental, economic, cultural, local, and international aspects in bolstering cyber security. The findings highlight the necessity of intensifying efforts to achieve comprehensive cyber security.

In Algeria, according to Abdelhamid (2020), cybercrime has escalated recently, underscoring the severity of the situation, especially as the country moves towards adopting an e-government approach. The study stressed the need for necessary security precautions to avoid cybercrimes. The Algerian military has established a "Cyber Defense and Systems Security Monitoring" unit to protect vital infrastructures from electronic threats.

Lastly, Bakri's study (2023) emphasized the dangers surrounding cyber security and ways to combat them. The study noted that Saudi Arabia ranks second globally in cyber security protection. It highlighted that cybercrime is among the top threats facing Gulf countries, including Saudi Arabia, the UAE, and Qatar, stressing the need for continuous vigilance to ensure cyber security.

Information security systems are crucial for protecting data in educational institutions, especially in the rapidly digitizing Arab countries. These systems enhance trust in the technological infrastructure, improving educational quality and developing organizational competencies (Al-Omari, 2022; Smith, 2023). Organizational learning capabilities are vital for achieving strategic objectives, with studies showing that they enhance institutions' adaptability to environmental and technological changes, contributing to competitive advantage (Jones, 2021). This study analyzes the impact of information

security systems on organizational learning capabilities in Arab educational institutions, using a descriptive analytical documentary method to evaluate these systems' effects on organizational competencies (Al-Qarni, 2023).

1-1-Statement of the Study:

Educational institutions in Arab countries face multiple challenges in effectively implementing information security systems. Studies indicate that these systems were initially aimed at protecting the economy, production, and security, and only later entered the realm of educational institutions (Al-Harbi, 2022).

1-2-Questions of the Study

1. How do information security systems impact organizational learning capabilities in educational institutions in Arab countries؟
2. How do educational institutions measure their organizational capabilities based on the available information security systems؟
3. What challenges do educational institutions face in effectively implementing information security systems؟

1-3-Objectives of the Study:

1. To analyze the impact of information security systems on organizational learning capabilities in educational institutions in Arab countries.
2. To evaluate how educational institutions measure their organizational capabilities based on information security systems.
3. To identify the challenges that educational institutions face in effectively implementing information security systems.

1-4-Significance of the Study.

- **Scientific Significance:**
  - The study contributes to the literature on the impact of information security systems on organizational learning in educational institutions.
  - It provides a theoretical framework that can be used in future studies to understand the relationship between information security and organizational learning capabilities.

- **Practical and Applicative Significance**
  - To provide practical recommendations for improving information security systems in educational institutions.
  - To assist decision-makers in developing educational policies that ensure information protection and enhance organizational learning.
  - To support educational institutions in developing effective strategies for implementing information security systems.
  - To raise awareness among staff in educational institutions about the importance of information security systems in improving organizational performance.

1-5-Definition of Key Terms.

- **Information Security Systems**: Systems designed to protect information and data from unauthorized access, disclosure, alteration, and destruction.
- **Organizational Learning:** The process through which organizations develop, enhance, and manage knowledge and standards to improve their capabilities.
- **Educational Institutions**: Schools, colleges, universities, and other establishments that provide educational services.

1-6-Study Limitations

This study focuses on educational institutions in Arab countries and examines the impact of information security systems on organizational learning capabilities. The study relies on data available in recent literature and official reports, which may face limitations related to data availability and recency.

2-Methodology

The researcher used the descriptive analytical documentary method to analyze the available data on information security systems and organizational learning capabilities in educational institutions. This includes analyzing previous studies, official reports, and relevant scientific articles.

2-1-Study Procedures

1. Collecting data from available sources such as previous studies and official reports.
2. Analyzing the data using the descriptive analytical method.
3. Evaluating the impact of information security systems on organizational learning capabilities.
4. Providing recommendations to improve information security systems in educational institutions.

3- Previous studies.

- **Al-Nuaimi (2024)** aimed to explore human and contextual factors influencing cybersecurity behaviors in organizations, particularly in higher education institutions. The study employed a systematic literature review methodology, analyzing multiple studies to develop a robust cybersecurity culture that supports sustainable development goals in cybersecurity training and education. Key findings provided an overview of human factors affecting cybersecurity, emphasizing their importance in higher education.
- **Mollah et al. (2023)** aimed to explore sustainable organizational performance in South Korea in the digital age by examining the impact of digital leadership on IT capabilities and organizational learning. The study involved an online survey of 173 employees and used structural equation modeling for analysis. Findings revealed that digital leadership significantly affects sustainable organizational performance, with IT-proactive stance and organizational learning fully mediating this effect, highlighting the role of digital leadership in enhancing IT capabilities and organizational learning.
- **Almuqrin et al. (2023)** aimed to explore the relationship between information system success and organizational sustainability in Saudi Arabian public institutions. The study collected self-reported data from employees at various government institutions and used correlation and regression analyses. Findings showed moderate implementation of organizational sustainability, with user satisfaction being the strongest predictor. The study emphasized the need for further research to identify other predictors of organizational sustainability.

- **Aseeri and Kang (2023)** investigated the impact of organizational culture and big data analytics (BDA) on strategic decision-making in Saudi Arabian universities. Using a quantitative cross-sectional survey methodology and PLS-SEM for analysis, the study found that organizational culture significantly impacts big data personnel (BDP) but not big data systems (BDS). Social and technical subsystems of BDA were significantly correlated with strategic decision-making, underscoring the importance of a data-driven culture and supportive management.
- **Saeed (2023)** aimed to explore information security awareness among computing students in Saudi Arabia. The cross-sectional study used an online questionnaire and factor analysis. Findings revealed that email and infrastructure management were significant factors in cybersecurity awareness, while password management and perception of security were not. Recommendations were made to improve cybersecurity awareness among students to prepare them for secure online practices.
- **Mustapha et al. (2023)** aimed to define critical success factors for knowledge sharing within academic institutions. Using a literature review and an online questionnaire, the study identified factors such as encouragement, acknowledgment, a reward system, fostering a knowledge-sharing culture, and leading by example. These factors were integrated into a framework for an Academic Knowledge Sharing System (AKSS).
- **Alegre et al. (2017)** aimed to investigate the relationship between transformational leadership and organizational learning capability with happiness at work in Spain's public health sector. The methodology involved an electronic questionnaire applied to a sample of 167 medical employees in allergy units. The study revealed that happiness at work could be measured using a new proposal and that transformational leadership predicts happiness at work through organizational learning capabilities. The study recommended that hospital directors and heads of allergy services consider the effects of transformational leadership to enhance happiness at work, emphasizing the need to create an atmosphere that fosters personal connections and enhances individual and organizational effectiveness.
- **Al-Busaidi & Olfman (2017)** aimed to investigate the impact of various factors on knowledge workers' intention to share knowledge through inter-organizational knowledge-sharing systems (IOKSS). The study utilized a survey methodology, though the exact sample size was not specified. The results showed that human factors significantly impact the intention to share knowledge through IOKSS, while system, organizational, and sector factors had indirect effects. This investigation is valuable for developing countries, where technological innovations like IOKSS are crucial for training, building human resources, and national knowledge management.
- **Rahman et al. (2016)** in Malaysia aimed to understand the antecedents of knowledge-sharing behavior among non-academic staff in higher learning institutions. Using a survey methodology, the study revealed that both attitude and subjective norms significantly and positively influence knowledge-sharing behavior, with the intention to share knowledge playing a crucial mediating role.
- **Berson et al. (2015)** aimed to determine how to design effective information security policies in organizations, focusing on employees' need for guidelines in decision-making. The methodology involved a survey and theories of utility and universality. The study found that clear, comprehensive, and easy-to-use policies are essential for effective information security, especially in exceptional cases. It recommended that policies be designed to provide clarity, flexibility.
- **Ayari (2014)** aimed to evaluate the information system of the Information and Communication Technology Department based on the ISO 27002 standard. The study used a descriptive analytical approach, collecting data through interviews, document analysis, and observation. Results indicated that 75% of security depends on personal skills and knowledge, with 25% on materials. The study emphasized the importance of the human element and organizational culture in achieving security goals.

- **Al-Saldi (2012)** aimed to identify the role of service quality dimensions and organizational learning capabilities in developing a culture of excellence in Kuwaiti industrial companies. Using a survey methodology, the study involved 105 managers from 27 companies. The findings showed a strong positive correlation between tangible service dimensions and the development of a culture of excellence, highlighting the importance of organizational learning capabilities.
- **Al-Omari (2012)** aimed to study the impact of information systems resources on achieving competitive strategies in Umniah Mobile Communications Company, Jordan. The study used a survey methodology with a sample of 30 employees across three administrative levels. Results indicated a high level of system resources availability and a significant impact of information systems resources on competitive strategies, except for growth strategies.
- **Siponen (2009)** aimed to present a vision for an information security awareness program to reduce user errors and improve the effectiveness of security controls. The study used a survey methodology and concluded that security techniques lose their benefit if misused or misinterpreted. It highlighted the necessity of awareness programs to reduce errors and enhance security control effectiveness.

The results of previous studies have shown a focus on information security, its usage difficulties, and the risks and challenges it faces in educational institutions. The researcher summarizes them as follows:

- Poor balance between clarity, comprehensiveness, and usability in security policies, as well as the complexity of balancing soft skills and material resources for security.
- Ambiguity in distinguishing between the impact of digital leadership across different organizational contexts, with difficulty in accurately measuring and promoting cybersecurity behaviors in higher education.
- Difficulty in accurately measuring happiness at work and knowledge exchange behavior.
- Difficulty in overcoming social, technical, and political barriers to effective knowledge exchange.
- Poor balance between the impact of information technology infrastructure and proactive attitudes on organizational performance, as well as the weakness of achieving comprehensive and consistent user satisfaction with information systems.
- Difficulty in overcoming cultural barriers to effective implementation of best practices for information systems.

On the other hand, the researcher believes that diagnosing the reality of information use and cybersecurity can lead to measures that achieve many benefits and practical applications:

1. Improving training and building human resources in cybersecurity for higher education institutions in Arab countries.
2. Benefiting from digital leadership to improve IT capabilities and organizational learning, and promoting a data-driven culture and supportive management to influence changes related to information security.
3. Developing targeted strategies to improve cybersecurity awareness among students.
4. Applying critical success factors to enhance the culture of knowledge exchange in academic institutions.
5. Enhancing leadership strategies to improve employee happiness and organizational effectiveness, while enhancing a better understanding of security procedures among users.
6. Developing effective practices and systems for knowledge exchange, by designing clear, comprehensive, and flexible information security policies.
7. Enhancing organizational culture to support security goals and excellence in information security, and encouraging positive attitudes and standards towards knowledge exchange.
8. Improving service quality and learning capabilities to enhance the culture of excellence.

Terms and concepts.

First: Information Security Systems:

Security is the set of rules, set by security officials in any place, which must be adhered to all people who can access it. The concept of security is broad and extends to all operations.

Entering, leaving, staying, or acting somewhere. Therefore, security in cyberspace includes rules and principles for controlling communication, transmitting information, and storing and preserving it. It also includes website security and security.

Electronic systems, in addition to communications security. That is, it is not limited to the physical meaning of security. That is, a guarantee that the information will not be destroyed, distorted, destroyed, or stolen, but also, a guarantee Its confidentiality, not being known to others, its credibility, and its validity. The relationship appears clear between information security and ensuring rights of access to data and system resources, through an identity verification mechanism and oversight that allows system users to be restricted to the group of people to whom this right has granted. (Jabour, 2012).

Second: Organizational Education:

It is the process of developing the capabilities and capabilities of the university institution in a way that achieves the institution's excellence and its adaptation to environmental changes, by employing expertise, advanced technologies, and renewable knowledge within the framework of a shared vision and teamwork, empowering members for education and preparing its requirements, and building an organizational culture that stimulates education, creativity, and knowledge innovation, to ensure continuity. The development and organizational excellence of the university. (Al-Janabi, 2016).

Third: Educational Institutions:

Universities are important educational institutions. It is located at the top of the educational ladder, and it falls on, Many responsibilities related to confronting society's problems, meeting its needs, and educating its members to achieve success, It presents it, which is the message that university Law in all countries works to achieve and stipulates what follows: "Universities are concerned with everything related to university education and scientific study carried out by their faculties its institutes to advance it culturally, aiming to contribute to the advancement of thought and the advancement of science and Developing human values". Universities include the intellectual and scientific elites of society and are no longer seen as a place, for Not only study but for it has also as a house of expertise for various sectors.(Al-Azzam & Al-Jadaiya, 2015) l

The following topics on the impact of the characteristics of information security systems on organizational learning capabilities in educational institutions which are as follows:

1- Information Security:

It is the protection of information and data circulated via the Internet from tampering, vandalism, and alteration, or from any danger that threatens it, such as the access of any unauthorized person to access it, tampering with its data, and reviewing it, by providing the necessary means and methods to protect it from internal and external risks, and the topic of information security is an old topic. However, the need and demand for it increased with the spread of the use of the Internet and reliance on it in all areas of life, which required the transfer of data and information across multiple networks. The spread of social media networks also provided an urgent need for this.

Information security is no longer an issue handled by technicians and technocrats within individual establishments and institutions in a fragmented manner.(Ghitas, 2007) Rather, it has become one of the issues undertaken by politicians,

strategists, and decision-makers, who translate it into national policies and strategies that work within the comprehensive national security system and control the relationship between information security and national security and its direction in Its correct path and a study by the researcher, and He divided the concept of information security into two basic parts: unilateral and dual.

Information security can be defined from three angles:

- From an academic standpoint: It is the science that studies theories and strategies to protect information from risks that threaten it and from activities that attack it.
- From a technical standpoint: it is the means, tools, and procedures that must be provided to ensure the protection of information from internal and external dangers.
- From a legal perspective: It is the subject of studies and measures necessary to ensure the confidentiality and integrity of the content and availability of information and to combat activities that attack it or exploit it to commit information crimes.(Hassan, D.T)

2-Characteristics of information security systems:

- **CONFIDENTIALITY:** This means ensuring that information is not revealed or accessed by unauthorized persons.
- **INTEGRITY: and integrity of content**: Ensuring that the information content is correct and has not been modified or tampered with, and in particular the content will not be destroyed, changed, or tampered with at any stage of processing or exchange, whether at the stage of internal dealing with the information or through illegal interference.(Wheeler, 2011)
- **AVAILABILITY:** Continuity of availability of information or service: Ensuring the continued operation of the information system and the continued ability to interact with the information and provide service to the information sites so that the user of the information will not be prevented from using it or accessing it. (Alnuaimy, 2020)
- **Non-repudiation**: The action related to the information by someone who has performed it: This means ensuring that the person who performed an action related to the information or its locations does not deny that he is the one who carried out this action so that there is the ability to prove that an action was carried out by someone at a specific time. Nonrepudiation assures that the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data. Further, this concept can apply to any activity, not just the sending and receiving of data; in a more general sense, it is a mechanism to prove that an activity was performed and by whom. Nonrepudiation is typically comprised of authentication, auditing/logging, and cryptography services. A common application of this service would be the digital signing of e-mail messages to prove that the purported sender sent the message received Since access control and nonrepudiation share so many common components, they are frequently implemented together in controls or else closely interrelated. For example, once an access control function has been performed, it may provide sufficient data to facilitate nonrepudiation or at least partial nonrepudiation data. (Al-Fathir & Al-Qahti, 2009).

3- What are organizational capabilities?

Organization capabilities (OC) are the strategic intangible assets that an organization relies on to get work done, execute its business strategy, and satisfy its customers.

These capabilities cannot arise from a single effort or by following an external model. Instead, they are sourced and refined internally from multiple interactions to be specific to educational organizations. It can include expertise, activities, information, knowledge, procedures, processes, skills, systems, technologies, or unique adaptive features. The strength and alignment of these assets define an organization's identity and differentiate it from competitors. Every organization develops

these traits and embeds them into its culture over time, so they are difficult for others to identify and replicate. For example, Coca-Cola could sell its soft drink formula to another company, but that company would not be able to emulate the same emotional connection that customers have with Coke. Building organizational capabilities is an indispensable part of the organizational development process. (Usrey, 2024).

4- Organizational learning capabilities:

Many researchers have emphasized the importance of organizational education as a process that has philosophical, cognitive, social, and technical dimensions that ensure the use of appropriate strategies to meet environmental requirements and enable organizations to act and think continuously to achieve the necessary adaptation to achieve goals by making gradual improvements or making radical changes to the knowledge base and organizational contexts. (Daham, 2005)

(Lee & Newman & Price, 1999:64) He emphasizes that it is necessary to pay attention to the impact of organizational learning capabilities in the decision-making process because it is linked to some external factors such as the environment, relationships, and rewards. (Lee et al., 1999).

5- Defining organizational learning capabilities:

Organizational learning capabilities are defined as the process of knowledge flow, which are those processes, characteristics, or constructs that enhance and help knowledge to be shared, acquired, and used effectively within or outside the organization. (Fan & Beh, 2024).They are organizational and managerial characteristics, practices, and skills, or factors That facilitate organizational learning processes, generating, acquiring, disseminating, and integrating information/knowledge, or allowing the organization to learn.(Huarng & Mas-Tur, 2016). Through the ability of managers within the organization to generate and circulate influential ideas, through generating and circulating ideas to Achieved. (Abubakar et al, 2019).

6- The importance of organizational learning capabilities:

Organizational learning is the process through which planned change is brought about in the organization and prepares it to be adaptable to changes in the environment surrounding it at the appropriate speed, by carrying out a set of operations, the most important of which is empowering individuals and investing previous expertise and experiences in facing and managing the future. Using knowledge and technology effectively to learn and improve performance, provided that this is done within the framework of an organizational culture based on the shared vision of the organization's members and supportive of work, collective learning, and continuous development, which enables these organizations to have the advantage of speed of learning and achieve their goals efficiently and effectively. For me, Individual learning is the process of assisting workers and people to acquire a wide range of skills and obtain a large amount of information. (Garcia-Morales & Llorens-Montes, 2006)

7- Dimensions of organizational learning capabilities:

Recent organizational learning literature indicates that each organization has its strategy and model, For organizational learning, consistent with the nature of its activities and objectives, the skills, capabilities, and experiences it possesses, and experiences, the educational level of its human resources, and the material and moral capabilities for practical practice, Organizational learning. However, three basic dimensions constitute the organizational learning process, which is divided, each dimension is a sub-dimension through which the three dimensions of organizational learning integrate and interact. (Goh & Richards, 1998)

Dimensions of Organizational Learning Capabilities:

1- Cognitive sharing:

Knowledge sharing is one of the important processes in knowledge management that leads to the exchange, dissemination, and distribution of knowledge between educational institutions and their employees, which reflects on their abilities, knowledge, and skills and thus increases their human efficiency to achieve the goals of educational institutions. (Bin Ibrahim, 2019) Through this, the importance of the knowledge-sharing process becomes clear to us. Moreover, benefit from it instead of becoming a prisoner in the minds of its owners. Sharing generates new knowledge through its exchange between members of educational institutions, which leads to the possession of an effective weapon for progress and advancement. This is what calls on organizations to pay attention to their knowledge resources and work to manage them through the processes of creating, storing, and sharing knowledge. Moreover, making optimal use of the individual experiences hidden in the minds and minds of individuals and transforming them into declared knowledge shared by all members of the organization so that it becomes of greater benefit and value. (Burnan, 2013)

Accordingly, interest in the concept of organizational learning has increased in business organizations as one of the modern administrative trends that organizations are currently seeking to meet environmental challenges. In light of this, organizational learning has become of great importance to researchers and practitioners because of what it provides to the organization and because of the strategic role, it plays in improving performance and achieving organizational excellence. (Bin Amra & Darban, 2020)

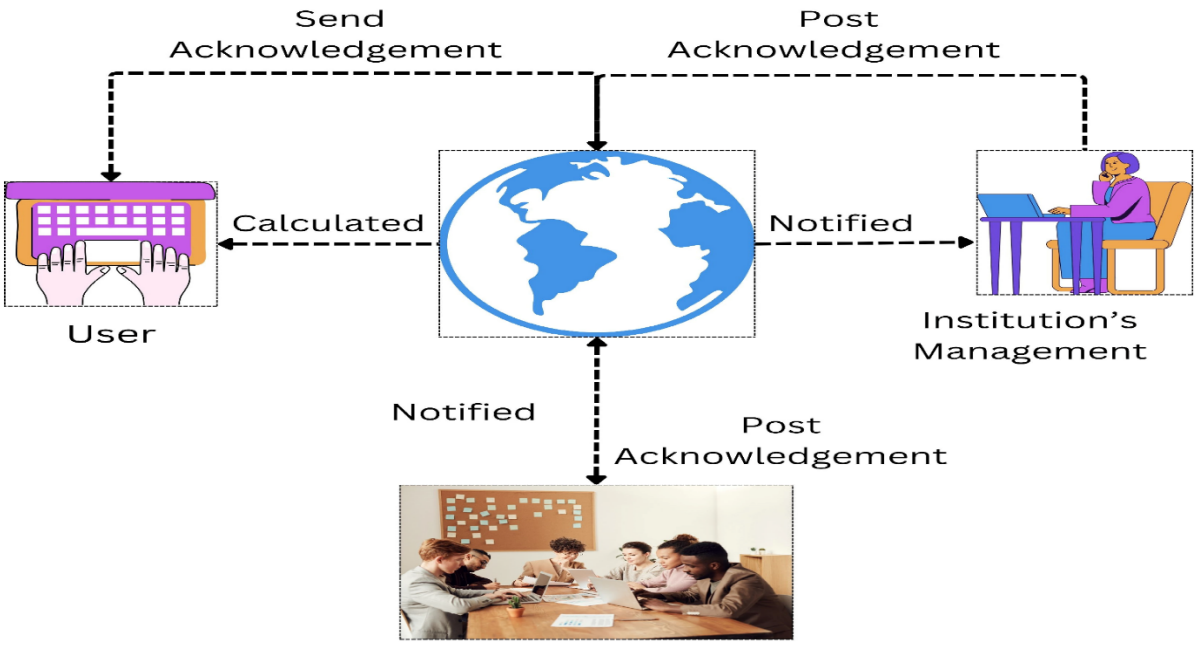
2- Organizational commitment:

Interest in the subject of organizational commitment began at the beginning of the second half of the twentieth century until the present time, as Hadi Salman specifically pointed out at the beginning of 1950. (Hadi, 2013) The concept of organizational commitment emerged, and despite the great interest in the phenomenon of commitment, in general, many studies and research were not able to provide a clear concept for its overlap with some other psychological and behavioral concepts. The first of these attempts is a proposal by Becker 1960 to develop a systematic concept for applying the behavior of individuals in organizations and taking actions that are consistent and compatible with maintaining survival. Backer called it the concept of Commitment, and it was the first attempt to establish a definition of commitment. Organizational. (Darwish, 2008)

Acknowledgement System Model (ASM) for Higher Education Institutions (HEIs)

Explanation:

The figure illustrates an Acknowledgement System Model (ASM) designed to stimulate knowledge-sharing behaviors in HEIs. It is based on a model proposed by (Mustapha et al, 2023)



(Mustapha et al, 2023)

The model highlights two acknowledgement pathways:

1. **User Acknowledgement:** Users can send non-monetary acknowledgments to the knowledge sharer.
2. **Institutional Acknowledgement:** The university management can send both monetary and non-monetary acknowledgments. Monetary acknowledgments could be determined based on the number of acknowledgments received from users (e.g., fellow academics, staff, and students). Non-monetary acknowledgments from the institution could include letters of appreciation or recognition.

This system aims to incentivize knowledge sharing by recognizing and rewarding those who contribute to the knowledge repository. (Mustapha et al, 2023).

Objectives of Information Security Systems in Educational Institutions

Daoud (2000, 48) pointed out that the security of information media is achieved through:

1- Providing an appropriate level for cylinders, magnetic tapes, and optical discs that contain the information.

2- Keep media containing backup copies of files in a remote location in danger.

3- Access to these media storage areas is restricted to authorized persons only.

4- Paying attention to destroying waste and debris such as cards and program lists using incineration ovens paper, paper lathe machines, etc. (Hassan, 2000)

Requirements for Achieving Information Security and Information Security Systems

In fact, there are important ways and means to reduce risks or reducing them and these methods:

- Proper construction of the information system is the right beginning for developing an effective strategy to monitor and evaluate the system and to protect the safety and integrity of its resources.

- Training users of the information system in the areas of information security, database security, and data security networks.

- Apply serious and strict measures to protect software and hardware from the first moment a system has operated the information. (Yassin, 2009)

4- Results of the Study.

4-1-Result of the question: "What is the level of impact of information security systems on organizational learning capabilities and performance of educational institutions in Arab countries؟

To answer this question, the researcher reviewed a summary of a set of studies that dealt with the impact of information security systems on organizational learning capabilities and the performance of educational institutions in Arab countries, and the researcher reviews them in order from the oldest to the most recent, as follows:

- **Al-Salloum et al. (2012)**. This study measured the impact of implementing management information systems on administrative work at King Saud University. It found that the university had the necessary infrastructure in place but needed specialized human resources, training, and support from senior leadership. Major obstacles included resistance to change and a lack of awareness about the importance of management information systems.
- **Ibrahim et al. (2018).**This study aimed to identify the impact of information security systems on organizational learning capabilities in Jordanian universities. The study revealed high levels of system availability and confidentiality, with a medium level of integrity. Information security systems significantly impacted organizational learning capabilities.
- **Al-Timani (2021).** The study examined the state of cyber security among individuals in Saudi Arabia from experts' perspectives. It highlighted that the government prioritized cyber security early on, even before the public recognized its importance. Common cybercrimes include electronic fraud, often due to low awareness and sharing personal information without understanding the risks.
- **Hamdan and Imran (2021)**. This research aimed to identify the role of information systems in the quality of administrative decision-making at Palestine Technical University. The study found a positive relationship between the implementation of management information systems and decision-making quality.
- **Al-Haimoudi (2023)**. The study emphasized the importance of cyber security in protecting personal data, corporate assets, and national security in Morocco. Cyber security plays a crucial role in shielding society from social engineering attacks and cyber threats targeting companies and the state.
- **Al-Janfaoui (2023)**. The study examined digital transformation and cyber security challenges in Kuwait from the perspective of academic police officers. The results indicated that the level of cyber security implementation in national institutions, including educational ones, was moderate, with no significant differences linked to age, educational qualifications, or work experience.
- **Tawfiq and Morsi (2023).** This study discussed the impact of electronic crimes in Egyptian society and the need for legislation and security guarantees. It emphasized cyber security as a strategic approach to protecting information, contributing to the digital transformation of institutions, including universities.
- **Amira (2023)**.The study explored the effectiveness of cyber security in the international educational system and its impact on regional and global communities. Educational institutions play a crucial role in enhancing cyber security, with recommendations for incorporating cyber security standards into educational curricula.
- **Mohamed (2023)**.This research focused on the impact of management information systems on decision-making quality at Nilein Bank. The results showed that management information systems improve decision quality by linking subsystems to the bank's overall objectives.

- **Sharaf Al-Din (2023).**The study aimed to assess the technical competencies of faculty members at the Faculty of Physical Education in light of digital transformation. The results indicated significant differences in technical competencies, recommending the inclusion of training courses to enhance these skills.

Key Points from the Previous Studies:

- **Importance of Cyber security:** Protects personal data and sensitive information and prevents cyberattacks.
- Community Awareness: The need to increase individual awareness about cyber security to reduce cybercrimes.
- **Digital Transformation Challenges**: Institutions need to improve digital transformation applications and manage cyber security effectively.
- **Technical Competencies**: Necessity to develop faculty members' technical competencies through training courses.
- Security Legislation: The need for laws and security guarantees to protect information in the digital age.
- Role of Educational Institutions: Enhancing cyber security in educational institutions to ensure continuous education.
- **Organizational Learning Capabilities:** Positive impact of information security systems on organizational learning capabilities.
- **Administrative Decision Quality:** Improving the quality of administrative decisions through management information systems.
- Infrastructure: The importance of having specialized infrastructure and software.
- **Training and Support**: Need for employee training and providing moral and financial support for effective implementation of information systems.

The Researcher's Commentary

The studies underscore the critical importance of information security systems in enhancing organizational learning capabilities and improving the performance of educational institutions in Arab countries. To maximize the impact, educational institutions should focus on several key areas:

- Strengthening Cyber security Measures: Prioritizing robust cyber security protocols to protect sensitive data and prevent cyber-attacks. This can foster a secure environment conducive to learning and innovation.
- Raising Awareness: Implementing comprehensive awareness programs to educate staff and students about the importance of cyber security, thereby reducing the incidence of cybercrimes.
- Improving Digital Transformation: Investing in advanced digital transformation initiatives that integrate cyber security measures. This can help institutions remain resilient against evolving cyber threats.
- Developing Technical Competencies: Providing continuous training and development opportunities for faculty and staff to enhance their technical skills, ensuring they are well-equipped to handle cyber security challenges.
- Establishing Security Legislation: Advocating for and implementing strong security laws and regulations to provide a framework for protecting information in educational settings.
- Enhancing Infrastructure: Ensuring the availability of specialized infrastructure and software that supports advanced cyber security measures. This involves regular updates and maintenance to keep systems secure.
- Fostering Organizational Learning: Leveraging information security systems to support organizational learning capabilities, which can lead to better decision-making processes and overall institutional performance.

4-2-How Do Arab Educational Institutions Measure their Organizational Capabilities Based on Available Information Security Systems؟

To answer this question, the researcher conducted a comprehensive review of the latest studies (2022-2024). By searching databases, it was found that educational institutions cannot do without Information Security Systems (ISS), especially given their increasing reliance on digital technology imposed by the current era. Evaluating organizational capabilities through ISS is crucial for ensuring data protection, compliance, and overall institutional integrity. (Rabii et al, 2020) study confirmed the uncertainty in the current state of information security maturity evaluation, highlighting that it has not yet matured and converged enough for a generic approach or many specific approaches to become the go-to choice. The methodology used was a systematic literature review to summarize existing research, identify gaps in the literature, and provide background for positioning new research studies. The tool employed was a systematic literature review. The relevant findings to the study's objective showed the prevalent influence of the ISO/IEC 27001/27002 standard but underscored the necessity for an in-depth investigation of ISO 21827. The study emphasized the implementation facet, noting a lack of implementation experiments compared to the number of proposed models, which could be due to the challenging task of validation and might explain the dominance of specific models.

Arab educational institutions measure their organizational capabilities based on information security systems through established frameworks like information Security Capability Maturity Model (ISCMM) and ISO/IEC 27001, custom assessments, and various tools and metrics. These methodologies provide a comprehensive understanding of the effectiveness of information security systems, helping institutions identify areas for improvement and ensure robust data security. Continuous evaluation and adaptation to these measures are essential for maintaining high standards of information security in an ever-changing digital environment.

4-3-Result of the question: "What are the challenges facing educational institutions in Arab countries in implementing information security systems effectively?

To answer this question, the researcher reviewed a summary of a group of studies that dealt with the challenges facing social institutions in Arab countries, including educational institutions, and the researcher reviews them in order from the oldest to the most recent, as follows:

- **Abu Zeid (2019).**This study on cyber security in the Arab world identifies three main dimensions: economic, information security, and general security. It highlights efforts by Arab countries to keep up with technological advancements and notes that Saudi Arabia leads in capacity building. The study underscores the need for further investment in cyber security, particularly in localizing technology and developing national capabilities.
- **Ahmed and Al-Dabbagh (2021).** This study from Iraq reports an increase in malware targeting networks, devices, systems, and applications, with ransomware being a significant threat. It proposes a machine learning-based system to protect Android smartphones from malicious apps by monitoring network traffic. The study finds that Decision Tree (DT) and extreme Gradient Boosting (XGB) classifiers perform best, with detection accuracies exceeding 99%.
- **Al-Kurdi.(2021)** This study in Palestine examines the state of cyber security and e-learning at An-Najah National University. It uses a survey methodology with 50 lecturers, finding significant differences in e-learning effectiveness based on lecturers' experience. The study reveals challenges in student culture and other areas but finds no significant differences in other comparative measures.

- **Kurtat .(2022)** This research investigates the impact of digital transformation challenges on scientific productivity among faculty members at Khamis Mushait Community College. Using a descriptive methodology and a survey distributed to 58 faculty members, the study finds a significant effect of digital research challenges on scientific productivity.
- **Abdel-Razek(2023) .**This study explores mechanisms to combat cybercrime in Saudi Arabia using a descriptive-analytical approach. It discusses the nature, characteristics, and motivations behind cybercrimes and highlights Saudi Arabia's efforts, including establishing the National Cyber security Authority, to protect its national interests.
- **Zhan et al, (.(2023** This study examines the role of perceived cyber security threats in the adoption of health information systems in Pakistan. It categorizes barriers into external attacks, employee factors, and technological factors, finding that external attacks and technological complexity are primary barriers, while employee factors have no significant impact.
- **Zhan et al, (.(2024** Building on the previous year's research, this study further investigates factors hindering the adoption of healthcare information systems (HIS). It reiterates that external attacks (e.g., phishing, ransom ware) and technological issues (e.g., complexity, vulnerability) are significant barriers, whereas employee factors are less impactful.

Identified Key Challenges:

1. **External Attacks:** Increasing prevalence of phishing, ransom ware, and other cyber threats.
2. **Technological Complexity**: Difficulty in managing and updating complex information systems.
3. **Inadequate Skills and Awareness**: Lack of cyber security skills and awareness among employees.
4. **Insufficient Investment:** Need for more investment in cyber security infrastructure and technologies.
5. **Rapid Technological Changes:** Keeping pace with fast-evolving cyber threats and technologies.
6. **Regulatory and Compliance Issues:** Challenges in adhering to varying cyber security regulations.
7. **Lack of National Capabilities:** Need for localization and development of national cyber security expertise.
8. **Data Protection:** Ensuring robust data protection mechanisms.
9. **Resource Constraints:** Limited resources for implementing comprehensive cyber security measures.
10. I**nter-organizational Coordination:** Need for better coordination among governmental and private entities.

The researcher believes that the identified challenges necessitate a concerted effort from various stakeholders to overcome. In particular, educational institutions in the Arab world require significant attention, as many policymakers may not fully appreciate the critical importance of cyber security in education compared to other sectors.

Tasks to Enhance Cyber security Awareness:

Table (1) Cyber Security Awareness Tasks for Students and Institutions (Saeed, 2023).

Student-Centric Tasks:	Institutional-Centric Tasks:
Concern for Application Security	Cyber security Training Programs for Students
Concern for Network Security	Institutional Security Policy
Concern for Operating System Security	Rewards/Punishments to Foster Secure Behavior among Students
Concern for Device Security	
Secure Browsing Practices	Events to Highlight Importance of Cyber security among Students
Secure Shopping Behavior	

Table (1) shows the division of cyber security tasks into student-centric and institutional-centric categories provides a comprehensive approach to enhance information security in educational settings. By addressing specific security concerns

and promoting best practices among students, while simultaneously implementing structured training programs and policies at the institutional level, educational institutions can create a robust cyber security culture. These measures are essential for safeguarding sensitive information and ensuring a secure online learning environment across the Arab world.

Activating Information Security Systems to Enhance Organizational Learning Capabilities in Educational Institutions in Arab Countries

An Analytical Background

Information security systems are essential for protecting sensitive data and information within educational institutions. These institutions face significant challenges in effectively implementing information security systems due to the continuous evolution of cyber threats, lack of resources, and training. Based on the current study and previous research, there is a critical need to develop information security systems in educational institutions in Arab countries to enhance organizational learning capabilities and address cyber security-related challenges.

Vision: "Leading information security systems that enhance the learning capabilities of Arab educational institutions and effectively address various cyber security challenges".

Mission: "We are committed to excellence and leadership in cyber security for Arab educational institutions by adopting cutting-edge technologies and security solutions, building a comprehensive data and intellectual property protection system, enabling innovative and secure learning environments, enhancing security awareness and culture, fostering strategic partnerships with governmental and private entities, and investing in cyber security research and development".

Values:

Figure (2) An Integrated Relationship. (By the Researcher)

1. Security: Ensuring data protection and system integrity against cyber threats.
2. Sustainability: Developing long-term, resilient information security practices.

3. Innovation: Integrating advanced technologies to enhance security measures.
4. Collaboration: Encouraging teamwork and partnerships for improved security.
5. Excellence: Striving for the highest standards in security performance.

Strategic Objectives:

1. Increase the Effectiveness of Information Security Systems in Educational Institutions in Arab Countries.
2. Improve and Develop Methods for Measuring Organizational Capabilities in Educational Institutions in Arab Countries.
3. Implement Procedures to Effectively Address Security Challenges in Educational Institutions in Arab Countries.

Operational Plan for Each Strategic Objective:

Strategic Objective 1: Increase the Effectiveness of Information Security Systems

Sub-goal	Activities	Responsible	Estimated Cost (USD)	Verification Indicators	Risk Management
Enhance Cyber security Techniques	1. Regular system updates. 2. Use advanced firewalls	IT Department	50,000	Number of updates. Quality of protection	Resource shortage
Develop Internal Security Policies	1. Draft new security policies. 2. Train staff on policies	HR Department	20,000	Number of new policies. Number of trained staff	Resistance to change

Strategic Objective 2: Improve and Develop Methods for Measuring Organizational Capabilities

Sub-goal	Activities	Responsible	Cost (USD)	Verification Indicators	Risk Management
Establish Standards for Security Performance Measurement	1. Develop new measurement standards 2. Conduct regular performance tests	Quality Department	30,000	Number of new standards Number of tests conducted	Lack of data
Use Advanced Analytical Tools	1. Purchase and install new analytical tools 2. Train staff on using tools	IT Department	40,000	Number of tools installed Number of trained staff	Additional costs

Strategic Objective 3: Implement Procedures to Effectively Address Security Challenges

Sub-goal	Activities	Responsible	Estimated Cost (USD)	Verification Indicators	Risk Management
Identify Key Security Challenges	1. Conduct regular threat analyses 2. Document discovered challenges	Cyber security Department	25,000	Number of analyses conducted Number of challenges documented	Lack of expertise
Provide Innovative Solutions to	1. Develop technical solutions 2.	IT Department	35,000	Number of solutions implemented Nu	Resistance to change

Overcome Challenges	Implement training programs			mber of training programs	

Recommendations for Success.

1. Strengthen partnerships with international institutions to improve security systems.
2. Allocate sufficient budgets for updating and developing security systems.
3. Provide continuous training programs for staff and students on cyber security.
4. Develop clear policies and procedures for handling security incidents.
5. Increase awareness of cyber security importance at the executive level.

Suggestions for Future Studies.

1. Study the impact of artificial intelligence technologies on improving information security systems in educational institutions.
2. Analyze the role of cooperation between educational institutions and security agencies in addressing cyber challenges.
3. Evaluate the impact of continuous staff training on the effectiveness of information security systems in educational institutions.

References.

1. Abdelhamid, A. (2020). The role of the National Defense System in achieving information security in light of the growth of cybercrime. Arab Journal of Informatics and Information Security, 1, 219-236. Retrieved from https://search.mandumah.com/Record/1169901/Description#tabnav
2. Abu Zaid, A. A. (2019). Cyber security in the Arab world: A case study of Saudi Arabia. Political Horizons, 48, 55-61. Retrieved from http://search.mandumah.com/Record/1018657
3. Abubakar, M. A., Elrehail, H., Alatailat, M. A., & Elc¸, A. (2019). Knowledge management, decision-making style, and organizational performance. Journal of Innovation and Knowledge. https://doi.org/10.1016/j.jik.2018.03.007
4. Ahmed, O. S., & Al-Dabbagh, O. A. I. (2021). A machine learning-based ransomware detection system. Journal of Education and Science, University of Mosul, 30(5), 86-102. https://doi.org/10.33899/edusj.2021.130760.1173. Retrieved from https://search.mandumah.com/Record/1203743/Description#tabnav
5. Al-Azzam, A. H., & Al-Jadaiya, M. N. (2015). The impact of transformational leadership on organizational learning in the Jordanian commercial banking sector in the northern region. Zarqa Journal of Humanitarian Research and Studies, 15(2), 30-40. https://doi.org/10.12345/zjhrs.2015.3040
6. Al-Fathir, K. S., & Al-Qahti, M. A. (2009). Information Security. Riyadh: King Fahd National Library Cataloging.
7. Al-Haimoudi, B. (2023). Cyber security and information systems protection. Journal of Jurisprudence and Law, 127, 64-107. Retrieved from http://search.mandumah.com/Record/1392001
8. Al-Janabi, H. (2016). The impact of organizational learning on organizational effectiveness: Applied research. Journal of Accounting and Financial Studies, 11, 166-185. https://doi.org/10.12345/jafs.2016.166185
9. Al-Kurdi, M. K. (2021). Cyber security and e-learning in Palestinian universities from the perspective of faculty members: An-Najah National University as a model. Arab Journal of Informatics and Information Security, 5, 103-123. https://doi.org/10.21608/jinfo.2021.201688. Retrieved from http://search.mandumah.com/Record/1189467

10. Almuqrin, A., Mutambik, I., Alomran, A., & Zhang, J. Z. (2023). Information system success for organizational sustainability: Exploring the public institutions in Saudi Arabia. Sustainability, 15(12), 9233. https://doi.org/10.3390/su15129233
11. AL-Nuaimi, M.N. (2024). Human and contextual factors influencing cyber-security in organizations, and implications for higher education institutions: a systematic review. Global Knowledge, Memory and Communication, 73(1/2), 1-23. https://doi.org/10.1108/GKMC-12-2021-0209
12. Alnuaimy, U. A. (2020). Criminal Liability Arising from the Violation of Information Security. Faculty of Law, University of Mosul. https://doi.org/10.12345/flum.2020.123
13. Al-Omari, G. I. (2012). The impact of information systems resources in achieving competitive strategies: A case study. Journal of Management and Economics, 34(90), 172-192. https://doi.org/10.12345/jme.2012.172192
14. Al-Salloum, O. I., Al-Huqbani, K. M., & Al-Ruwaili, A. A. (2012). The impact of management information systems on administrative work: A field study at King Saud University. Journal of the Institute of Public Administration in Saudi Arabia, 353-397. https://doi.org/10.36715/0328-052-003-001
15. Al-Timani, M. Z. A. (2021). The reality of information awareness of cyber security among individuals in Saudi society as perceived by cyber security experts. Journal of Social Work, 67, 1-23. Retrieved from http://search.mandumah.com/Record/1195996
16. Amira, M. Z. A. (2023). Cyber security and the international education system. Ain Shams University Journal of Reading and Knowledge, (260), 55-96. Retrieved from https://search.mandumah.com/Record/1387559/Description#tabnav
17. Bakri, S. A. H. (2023). Cyber security protection and the Gulf Cooperation Council: Six axes for the work of the Saudi National Cyber security Authority provide a secure Saudi cyberspace. Gulf Opinions, 184, 37-42. Retrieved from http://search.mandumah.com/Record/1449792
18. Bin Amra, A., & Darban, A. (2020). The impact of knowledge sharing in enhancing organizational learning. Leadership Journal of Business Economics, 6(3), 40-57. https://doi.org/10.12345/ljbe.2020.4057
19. Bin Ibrahim, M. A. (2019). The impact of organizational trust on knowledge sharing behavior. (Master's thesis, Muhammad Kheidar University).
20. Burnan, H. (2013). The impact of organizational climate on knowledge sharing. (Master's thesis, Muhammad Kheidar University).
21. Ciampa, M. (2005). Security+ Guide to Network Security Fundamentals. Thomson Course Technology.
22. Daham, A. S. (2005). Organizational learning and its impact on the success of organizations: A field study in the companies of the Ministry of Construction and Housing in Iraq. (Master's thesis, University of Baghdad).
23. Daoud, H. T. (2000). Information Systems Crimes. Naif Arab Academy for Security Sciences, Studies Center and Research.
24. Darwish, M. A. (2008). The Theory of Organizational Commitment. Alam al-Kutub.
25. Fan, Z., & Beh, L. S. (2024). Knowledge sharing among academics in higher education: A systematic literature review and future agenda. Educational Research Review. https://doi.org/10.1016/j.edurev.2024.100012
26. Garcia-Morales, V. J., & Llorens-Montes, F. J. (2006). Antecedents and consequences of organizational innovation and organizational learning in entrepreneurship. Industrial Management and Data Systems, 106(1), 21-42. https://doi.org/10.1108/02635570610641097
27. Goh, S., & Richards, G. (1998). Benchmarking the learning capability of an organization. European Management Journal, 15(5), 525-583. https://doi.org/10.1016/S0263-2373(98)00036-8
28. Hadi, A. S. (2013). The Role of the Contemporary Leadership Style in Achieving Organizational Commitment: An Analytical Study of the Opinions of Senior Managerial Leaderships in Iraqi Industrial Companies. St Clements University.
29. Hamdan, R. A., & Imran, M. (2021). The role of information systems in the quality of administrative decision-making at Palestine Technical University from the perspective of administrative staff. Arab Journal of Scientific Publishing, (2), 372-400. Retrieved from https://search.mandumah.com/Record/1435516
30. Hassan, F. F. (n.d.). An introduction to information security and an introduction to electronic crimes and how to protect and optimal use of available resources to reach the maximum levels of protection in ministerial departments. Ministry of Interior, Directorate of Information Technology, Training and Development Department, Studies and Research Division.

31. Huarng, K., & Mas-Tur, A. (2016). New knowledge impacts in designing of implementable innovative realities. Journal of Business Research, 69(5), 1529-1533. https://doi.org/10.1016/j.jbusres.2015.10.111
32. Ibrahim, S. B., Al-Amin, A. M., & Awadallah, A. H. (2018). The impact of information security system characteristics on organizational learning capabilities in Jordanian universities. Journal of Economic, Administrative and Legal Sciences, 2(12), 1-25. https://doi.org/10.26389/AJSRP.E130718
33. Jabour, M. A. (2012). Security in Cyberspace: Information Security and Legal Security.
34. Kartat, R. M. (2022). The impact of digital transformation obstacles on scientific research productivity of faculty members at the Community College in Khamis Mushait. Journal of Amman Arab University for Research- Educational and Psychological Research Series, 7(1), 518-531. Retrieved from http://search.mandumah.com/Record/1221341
35. Kurdi, M. K. (2021). Cyber security and e-learning in Palestinian universities from the perspective of faculty members: A case study of An-Najah National University. Arab Journal of Informatics and Cyber security, (5), 103-123. https://doi.org/10.21608/jinfo.2021.201688. Retrieved from http://search.mandumah.com/Record/1189467
36. Lee, D., Newman, P., & Price, R. (1999). Decision Making in Organizations. Prentice-Hall.
37. Maurer, U. (2004). The Role of Cryptography in Database Security.
38. Mohamed, N. A. A. (2023). The impact of management information systems on the quality of administrative decisions in commercial banks: A case study of the Nilein Bank Group- Sudan during 2010-2022. Kalzim Journal of Applied Studies, (4), 7-32. Retrieved from https://search.mandumah.com/Record/1424351
39. Mollah, M. A., Choi, J.-H., Hwang, S.-J., & Shin, J.-K. (2023). Exploring a pathway to sustainable organizational performance of South Korea in the digital age: The effect of digital leadership on IT capabilities and organizational learning. Sustainability, 15(10), 7875. https://doi.org/10.3390/su15107875
40. Mustapha, S. M. F. D., Syed, E., Evangelista, E., & Marir, F. (2023). Towards designing a knowledge sharing system for higher learning institutions in the UAE based on the social feature framework. Sustainability, 15(22), 15990. https://doi.org/10.3390/su152215990
41. Rabii, A., Assoul, S., Ouazzani Touhami, K., & Roudies, O. (2020). Information and cyber security maturity models: a systematic literature review. *Information and Computer Security, 28*(4), 627-644. https://doi.org/10.1108/ICS-03-2019-0039
42. Rahman, M. S., Osmangani, A. M., Daud, N. M., & Abdel Fattah, F. A. M. (2016). Knowledge sharing behaviors among the non-academic staff of higher learning institutions: Attitude, subjective norms and behavioral intention embedded model. Library Review, 65(1/2), 65-83. Available at: www.emeraldinsight.com
43. Saeed, S. (2023). Education, online presence and cyber security implications: A study of information security practices of computing students in Saudi Arabia. Sustainability, 15(12), 9426. https://doi.org/10.3390/su15129426
44. Sharafeddin, M. S. A. (2023). Technical competencies of faculty members at the College of Physical Education in light of the trend towards digital transformation. Beni Suef Journal of Physical Education and Sports Sciences, 6(11), 161-189. Retrieved from https://search.mandumah.com/Record/1369821
45. Siponen, M. (2009). Information security management standard: Problems and solutions. Information & Management, 46, 267-270. https://doi.org/10.1016/j.im.2009.05.002
46. Tawfiq, S. M., & Morsi, S. E. (2023). Requirements for achieving cyber security in Egyptian universities in light of digital transformation from the perspective of faculty members: A case study of Benha University. Sohag University Journal of Education, (105), 737-861. https://doi.org/10.21608/edusohag.2023.283004.
47. Yassin, S. G. (2009). Management Information Systems (Arabic Edition). Al-Yazouri Scientific Publishing House.
48. Zhan, Y., Ahmad, S. F., Irshad, M., Al-Razgan, M., Awwad, E. M., Ali, Y. A., & Ayassrah, A. Y. B. A. (2024). Investigating the role of Cyber security 's perceived threats in the adoption of health information systems. Heliyon, 10(1), e022947. https://doi.org/10.1016/j.heliyon.2023.e22947