Migration Letters

Volume: 21, No: S7 (2024), pp. 593-611

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

Requirements And Challenges Of Achieving Cybersecurity From The Point Of View Faculty Members

Nesreen Abdou Elhadiede

Abstract:
The study aimed to identify the requirements for achieving cybersecurity at the University of Hail from the point of view of faculty members, as well as to identify the challenges that prevent the achievement of these requirements. The study relied on the descriptive approach to suit the nature of the study, and used the questionnaire as a tool for collecting data. The study sample consisted of (343) of faculty members in various fields from university colleges, the study concluded that the faculty members agreed that the University of Hail's need for requirements to achieve cybersecurity is high, the first of which is the human requirements. The study found that there were many challenges facing achieving cybersecurity at the University of Hail, most notably the lack of an approved strategy for cybersecurity at the university and the lack of standards. The study recommended that the University of Hail should work to provide cybersecurity requirements and reduce the challenges facing it.

Key words: *Cybersecurity, Cybersecurity requirements, University of Hail, Challenges*.

Introduction:

Today the world is undergoing rapid changes in all areas of life, most notably technology. The effects of this development have been reflected in the work environments, which required making many adaptations to the me[1]thods and style of work. Employing modern technologies in work environments has become something that imposes itself on the work system, and this has been accompanied by many challenges including maintaining intellectual property rights, information security and confidentiality. In light of the digital revolution that is specific to specializations, and which imposes itself on all periods of life, especially the education sector; This is carried by the Columbia Express Company through the Internet, the diversity and spread of means of communication, in addition to the diversity of sources from which information is obtained (Al-Montashri and Hariri, 2020). With the digital transformation that the world is witnessing, which has created dominance in all educational, educational, technological, economic and political fields, which requires countries to keep pace with the rapid spread of technology and be prepared to confront the challenges posed by this spread, control those technologies and raise readiness to confront cybercrimes, as global cyber threats have increased which threatens personal and global security at the same time (Al-Aqlaa and Ali, 2022).

The rapid digital development has been accompanied by the emergence of many cybercrimes that were not known before, due to the availability of digital technologies and the ease of obtaining them as well as their low cost, the possibility of concealment and working comfortably through them, and the ease of communication between different categories and groups in different parts of the world, which facilitated the penetration of various Systems,

Assistant Professor of Educational& Information Technology, Computer Science and Engineering, University of Hail, KSA.

whether in military, financial, or educational institutions, harm them or disrupt the services they provide (Al-Timani, 2021).

The issue of cybersecurity is one of the issues that has occupied the attention of governments and institutions in various countries of the world, with the increase in dangerous practices and criminal acts through digital technologies and the Internet, which requires institutions to keep pace with digital development and pursue the digital transformation to confront the security and social challenges that are now threatening cyberspace institutions and the state as a whole (Riley, 2022). With the increase in electronic attacks in light of digital transformation, which has made the Kingdom of Saudi Arabia more keen on achieving the security of data and digital operations, and providing strong security systems capable of confronting any electronic attacks, and in line with the Kingdom's Vision 2030, the National Guidance Center for Cybersecurity launched guides to raise the level of awareness of cyber security, avoiding cyber risks and reducing their impact, and launching awareness campaigns (National Cybersecurity Guidance Center, 2023).

In this field, the Ministry of Communications and Information Technology, in cooperation with the Human Resources Development Fund, launched an initiative entitled "The National Cybersecurity Academy," which seeks to raise the level of national digital capabilities in various fields of digital technology in response to the requirements of digital transformation. This initiative includes several tracks, including data analysis, Artificial intelligence, web development and its applications, design and development of electronic games and others (Human Resources Development Fund, 2021). To activate the role of educational institutions in spreading the culture of cyber security, the Ministry of Education and the National Cybersecurity Authority signed an agreement to enhance joint cooperation in the field of education, scientific research and awareness in the field of cyber security. This included joint cooperation in higher education programs, building capabilities in the field of cyber security, and raising the quality of outputs. Education programs in the field of cyber security, and increasing awareness of cybersecurity in education (Ministry Of Education, National Cybersecurity Authority, 2021).

Many studies have addressed the importance of cyber security, as cybersecurity is considered a mechanism for confronting fraudulent attacks and reducing their risks. The study conducted by (Zaqout et al., 2022) emphasized the importance of educating faculty members about the importance of cybersecurity in light of digital transformation.

(Al-Alfi, 2010) indicated that the importance of cybersecurity is due to the need to develop a national strategy and protect the state's infrastructure and institutions to preserve and protect information, and deter electronic crime, in addition to protecting intellectual property, secrets, and trademarks. (Al-Bishi, 2021) explained that cybersecurity affects the promotion of digital culture, and stressed the necessity of providing cybersecurity requirements and its applications, and focusing on information protection and security programs because they have an impact on the confidence of the digital beneficiary, many studies have indicated, including the study of (Al-Qahtani, 2019).

(Al-Jundi and Mohammad, 2019) indicated that there is a major movement in the entire world towards information security, networks and cyber security, by joining agreements to combat cybercrime, and educational institutions also focus on making the most of information and communication technology while protecting their systems in order to preserve the confidentiality of their data and protect networks, systems, and is moving towards adapting its policies and raising awareness of educating employees about cybersecurity requirements.

It is clear that defining the requirements for achieving cybersecurity and studying the challenges that prevent achieving those requirements has become an indispensable obligation. In light of the above, it is clear that there is a need to determine the requirements for achieving cybersecurity at the University of Hail from the point of view of faculty members, and studying

the obstacles and challenges that limit the effectiveness of employing cybersecurity requirements at the University of Hail.

Study Problem:

After the spread of the Corona pandemic crisis (Covid-19), and the digital transformation that the world has witnessed, especially the education sector, electronic attacks against institutions have increased, and many electronic crimes have emerged that did not exist before. All of this has made it necessary to confront these attacks and provide protection. necessary, and effectively activate the application of cyber security, and at the same time raise the level of awareness of the requirements of cyber security, and the mechanisms for its activation, to rely on technical and digital systems in its policies and administrative and academic programs as part of its endeavor to keep pace with the rapid developments around it and to achieve the goals of the (Kingdom's Vision, 2023), which resulted in the flow and exchange of a huge amount of information and data within these universities, and in light of global developments and the increase in electronic crimes, digital transformation needs protection measures. (Richardson, and Waller, 2020) showed that the Cybercrime targets institutions that do not have a culture of cyber security, which emphasizes the importance and necessity of cyber security, especially in light of the requirements of digital transformation.

There is a close connection between achieving cybersecurity and the level of awareness of workers in various institutions about those requirements, and this confirms the importance of raising the level of awareness of cybersecurity and its requirements. Hence the idea of the current research came, which is to study the level of awareness of faculty members at the University of Hail about cybersecurity requirements, and the challenges facing members of faculty were prevented from hiring cybersecurity requirements. In light of the above, the problem of the current research crystallizes in the need to determine the requirements for achieving cybersecurity at the University of Hail from the point of view of faculty members, and the challenges that prevent the activation of cybersecurity requirements.

Study Questions:

In light of the above, the research questions are determined in the following main question**:"What are the requirements for achieving cybersecurity at the University of Hail from the point of view of faculty members and what are the challenges facing this?"**

The following main questions branch out from the previous main question:

1- What are the cybersecurity requirements at the University of Hail from the perspective of faculty members at the University of Hail?
2- What are the challenges facing faculty members at the University of Hail in activating the requirements for achieving cyber security?

Study Aims:

The study aims to determine the requirements for achieving cybersecurity at the University of Hail from the point of view of the university's faculty members, and to study and identify the challenges faced in achieving cybersecurity requirements at the University of Hail.

Study Importance:

The importance of the current study is in trying to determine the requirements for achieving cybersecurity from the point of view of faculty members at the University of Hail, as activating cybersecurity requirements in the educational system has become an indispensable obligation. As well as searching for an attempt to overcome the security obstacles facing the requirements for cyber activation.

Study limitations:

The current research is limited to achieving its objectives within the following limits:

Objectivity border: Requirements for achieving cybersecurity at the University of Hail and the challenges of achieving those requirements.

Spatial limitations: University of Hail.

Temporal limits: The first semester of the academic year 2023.

Human limits: Sample of faculty members at the University of Hail.

Study Methodology:
The current study relied on the descriptive approach and analysis phase to determine cybersecurity requirements, measure the level of awareness of faculty members at the University of Hail about cybersecurity requirements, and identify the challenges that prevent the activation of cybersecurity requirements.

Study literature:

Cybersecurity: Known by the (National Cybersecurity Authority, 2018) it is the protection of networks, information technology systems, the services they provide, and various operational technology systems and their components its hardware and software components, and the data it contains, are protected from any hacking, disruption, modification, illegal use or exploitation. (Al-Rukban, 2023**)** defines it as the administrative and technical procedures and processes used to protect administrative information systems from any attack, hacking, disruption, or misuse.

It is defined operationally in the current study as: A set of technical procedures and processes used to protect information systems at the University of Hail against any attack, hacking, or misuse.

Cybersecurity concept: The concept of cybersecurity is broad and comprehensive; it includes securing data and information that are exchanged and circulated in various institutions, whether inside or outside them, and that data is stored on servers in various bodies, and cybersecurity works to protect it from penetration, and the concept of cybersecurity coincides with the digital revolution that imposes itself on the electronic security of humans. (Zaqout et al., 2022) refers to cybersecurity "A security concept that protects information and the processes and technologies related to the information, not any type of unwanted access or use of that information indefinitely". (Tawfiq and Al-Morsi, 2022) defined cybersecurity as: “All procedures, technical means, measures and efforts that Benha University should provide to its faculty members, with the aim of protecting various sources (software, mobile devices, and personal digital data) from transgressions, illegal interference, resisting hacking attempts or unexpected incidents, and enhancing Its privacy and encryption, and taking measures to protect faculty members from the dangers of cyberspace.”

Types of cybersecurity: There are multiple types of cyber security, including:
1- **Network security**: It is related to protecting computers from hacking attempts and attacks that may be exposed to them, whether inside or outside the network, as a firewall was used to protect devices from hacking.
2- **Application security**: This relates to the mechanism for protecting data and parameters on programs and applications on the computer, such as password, authentication processes, etc.

3- **Cloud security**: related to protecting data and information saved on cloud programs.
4- **Operational security**: related to internal cybersecurity risk management; where experts are employed to manage risks, alternative plans are developed in the event of cyber attacks, and it is concerned with raising the level of employees' awareness of cybersecurity and training them on best practices to avoid risks.
5- **Internet of things security**: is concerned with setting security policies in the network infrastructure with the aim of assessing and reducing the potential risks of various Internet of Things (IoT) devices.
6- **Data security**: Data security works to protect data during transmission and at rest through an effective storage system and secure data transfer (Tawfiq and Morsi, 2023).

Cybersecurity objectives:

(Al Samhan, 2020; Al-Bishi, 2021) Indicated for cybersecurity objectives in the following points:
1- Protecting the technical and operational infrastructure at all levels from electronic attacks.
2- Air and attack lines do not use red and information lines.
3- Providing a safe and reliable environment for dealing in the information society.
4- Providing a highly efficient infrastructure to confront electronic attacks.
5- Eliminating weak points in various institutions through which institutional systems can be hacked.
6- Educating individuals and workers in various community institutions about cybersecurity and how to achieve it.
7- Determine the readiness and readiness of state institutions to employ and activate cybersecurity requirements.

Dimensions of cyber security: one of the most important dimensions of cybersecurity is what it refers to (Al-Haddad, 2022):
1- **Military Dimensions**: Diversity in the system's ability to partially link all its criminal units, including allowing the exchange of information quickly, accurately, and security of military precision in a timely manner, greatly affecting cyber Jackson, which includes world security and leads to wars and conflicts between countries**.**
2- **Political dimensions**: it aims to protect the state's political system and preserve its entity. Technologies can be used to broadcast information that leads to destabilization and security of the country.
3- **Economic dimensions**: There is a close connection between the economy and knowledge. Most countries rely on the exchange of knowledge and information to strengthen and prosper their economy, which confirms the role of cybersecurity in protecting the knowledge economy from theft and fraud.
4- **Legal dimensions**: In light of the transformation to the digital society, a set of new laws have emerged that are compatible with the developments of the times and that are linked to the regulatory and legislative environment regulating the protection of the information society and the preservation of rights in it, and the role of cybersecurity here is to work to apply and implement these laws and legislation.
5- **Social dimensions**: In light of the knowledge society, it has become possible for every individual in society to express his opinion, disseminate his ideas, and access various information and various cultures without restrictions and from here comes the role of cybersecurity in protecting and preserving the values and identity of society.

From the above, it is clear that cybersecurity requirements must be available and implemented in order to reduce attacks and cybercrimes that threaten the security and stability of society and work to destroy the society's identity and culture.

Literature Review:

Over the past years ago, many studies utilized the cybersecurity; this section is overviews the recent empirical analyses using the cyber security. The study of (Mihci and Kiliç, 2019) aimed to determine the level of awareness of each of the secondary school students, teachers, and parents about the requirements of cyber security, and to determine the level of knowledge and skills of the research sample towards cyber security. The study relied on the survey method, and the study sample consisted of (6839) students, (749) teachers and (4916) guardians. The study used an electronic questionnaire to collect data in seven educational regions. The study found that the level of students' awareness of cybersecurity requirements is high, especially with regard to Internet addiction, online privacy, and copyright. The study found that there is a discrepancy among students in the level of awareness according to the variable of gender and level Education, rate of Internet use, and desire for e-learning. As for the level of teachers' awareness of cybersecurity requirements, it was average with regard to all cybersecurity concepts and requirements. As for parents, their level of awareness of Internet requirements was moderate, especially with regard to Internet addiction, online privacy, inappropriate online content, and copyright. Parents scored a level of High awareness regarding cyber bullying.

(Riley, 2022) aimed to identify the best cybersecurity practices in educational institutions that are used in public education schools. The study sought to identify the obstacles that prevent the achievement of cybersecurity principles in public education schools in the state of Texas, and to identify the best practices to confront Electronic attacks throughout the state. The study used a questionnaire tool to collect data. This study included 381 schools. The study relied on the descriptive approach. The study concluded that the cybersecurity legislation in force in public education schools is among the best practices for cyber security. The study indicated that the role of the coordinator Cybersecurity does not affect the level of cybersecurity awareness in general education schools. The study suggested transferring the role of cybersecurity awareness to an executive position within the school that works to raise the level of awareness of cybersecurity requirements. This study indicated that one of the most important obstacles facing the implementation of cybersecurity in schools is the lack of a budget dedicated to cybersecurity and poor financial support.

(Dawson, et, al., 2022) showed that the level of awareness of pre-service teachers in the field of cybersecurity and studying the effect of specialization and gender on the level of awareness of pre-service teachers in cyber security. This study relied on the descriptive analytical approach, and the study used the questionnaire as a tool for the study, and the study sample was from a random sample of pre-service teachers, the study found that the level of awareness of pre-service teachers in the field of cybersecurity was weak. The study confirmed that there were no differences in the level of awareness in the field of cybersecurity according to the variable of specialization and gender. The study recommended the need to make efforts to prepare pre-service teachers and qualify them to integrate learning. This study showed that the Cybersecurity from various curricula, and the study presented Vision 2025, which aimed that by the end of 2025, all pre-service teachers will be qualified to integrate cybersecurity concepts into various curricula according to the academic level of students.

(Al-Manea, 2022) identified the reality of achieving cybersecurity in Saudi universities in light of Vision 2030. The study was followed by a descriptive and analytical class, and the questionnaire was adopted as a computer tool. The number of staff reached (210) employees of the Saudi Thirties Mosque, namely: (Umm Al-Qura University, (Imam Abdul Rahman bin

Faisal University, Imam Muhammad bin Saud Islamic University). The study concluded that the sample members agreed to a moderate degree with the reality of achieving cybersecurity in Saudi Arabia in Vision 2030. It was found that the sample members agreed with a very strong degree of resistance to the obstacles to achieving cybersecurity in Saudi universities in light of Vision 2030. This study showed the most important of these obstacles is the low level of experience among employees, and the weakness in cooperation between skills employees in universities to achieve cyber security.

(Zaqout et al., 2022) aimed to identify the degree of awareness of faculty members in Libyan universities about the importance of cybersecurity in light of digital transformation, specifically at Zawia University. This study relied on the descriptive and analytical approach, and they used the questionnaire as a tool for collecting data. The study sample consisted of 138 faculty members at Zawia University, and the study reached the following conclusions where: the level of awareness of faculty members at Zawia University about the importance of cybersecurity was very high, and the study recommended holding training courses for faculty members on cyber security, and conducting workshops periodically to follow up on cybersecurity developments.

(Farag, 2022) explained the reasons for digital cyber culture in the digital transformation of the university, by (Sattam bin Abdulaziz) and to determine the differences in the view of the sample members regarding the reasons for digital cyber culture in the digital transformation of the university according to the variables: “college, specialization, and years of experience.” Therefore this study used a descriptive model and designed a questionnaire consisting of (26) items distributed across three sectors. The study began with (125) members, and concluded that the reasons for promoting cyber culture in light of the digital transformation to (Sattam bin Abdulaziz) from the point of view of the members, the faculty received an average score of (3.55) with a moderate degree of resistance, and it is the focus of community efforts to enhance the culture of cybersecurity at the university’s highest digital level with an average of about (3.70), followed by the focus of pioneering motivation in enhancing the culture of cybersecurity at the university to an overall average of about (3.51), and the focus of the technical reasons had an average score of about (3.46), and it showed that there were no statistically significant differences depending on the college variable and academic rank, while there were differences due to the years of experience variable.

(Al-Aqlaa and Ali, 2022) aimed to reveal awareness of cyber concepts among computer teachers in the city of Hail, and the study relied on descriptive security drawings. The smart study included (184) computer teachers in the middle and secondary schools in Hail. The electronic questionnaire study has already begun, to deduce the study to the degree of cognitive awareness and computer parameters in the city of Hail, including cybersecurity to medium, and the study reached to know their awareness in brief ways on the cybersecurity system to medium, and reached to study the presence of statistically significant differences in the cognitive parameter and computer parameters in cybersecurity due to the variable gender of female teachers: There was a study of statistically significant differences between the level of middle school and high school teachers in cyber security, and there was no statistically significant differences in the awareness of computer teachers in cybersecurity concepts due to the variable of experience or academic qualifications, while there were Statistically significant differences in the cognitive parameter and the computer parameters regarding the concepts of cyber law due to the students’ variable, and they were asked to respond one or more.

(Al Habib, 2022) aimed to identify the degree of awareness of cybersecurity concepts, the degree of awareness of cybersecurity requirements, and ways to enhance awareness of among male and female graduate students at the College of Education at Imam Mohamed bin

Saud Islamic University. The study relied on the descriptive approach, and used the questionnaire as a tool for the study. The study sample consisted of (269) male and female students. The study found that the study sample's level of awareness of cybersecurity concepts was high, and they had a high degree of awareness of cybersecurity requirements. The study showed that the study sample's approval of ways to enhance awareness of cyber security. The study recommended activating the College of Education for procedures to raise awareness of cybersecurity for graduate students.

(Tawfiq and Morsi, 2023**)** aimed to identify the requirements for achieving cybersecurity at Benha University in light of digital transformation from the point of view of faculty members, by reviewing the concept of cyber security, its origins, dimensions, goals, and importance, and identifying the most important requirements for achieving cybersecurity in Egyptian universities in light of digital transformation, and the most important obstacles that prevent achieving these requirements from the point of view of the faculty members at Benha University. The study relied on the descriptive approach to achieve its objectives, and used as a tool to collect data on the most important requirements for achieving cybersecurity at Benha University in light of digital transformation. The study sample consisted of 248 faculty members, and the study reached an agreement. A sample of the requirements for achieving cybersecurity at Benha University in light of digital transformation, which represented a set of technical, material, human and cognitive requirements, and obstacles to achieving cybersecurity requirements at Benha University.

(Hong et al., 2023) aimed to identify the different elements that exist on the level of awareness of cyber security, as well as the effect of studying the difference in each of (educational level - gender and type of work (full-time - part-time)) for individuals to determine the study on their level of awareness of security. The technical study was conducted from 852 students, 325 female students, and 475 employees across two cities in China. The study relied on analytical descriptive models. The questionnaire tool was developed as a remote sensing tool from three axes. The study concluded that there is a discrepancy in the level of awareness of cybersecurity for some researchers, there is a need to study statistically significant differences in the average cyber awareness according to the variable of specialized educational qualifications in postgraduate studies, as well as the existence of statistically significant differences in the average cyber awareness according to the nature of work variable (full - partial) due to complete specializations. This study showed that is not the existence of significant gender differences was determined according to the difference in the level of awareness of cyber security.

(Gümüş, et al., 2023) aimed to identify the level of pre-service teachers' awareness of the requirements of cybersecurity and digital data security to know their perceptions about digital ethics. The study relied on the descriptive approach and used the electronic questionnaire as a study tool to collect data and consisted of three axes: "Awareness of cyber bullying", the security of the digital data and the ethics used information and communication technologies. The study sample consisted of (879) pre-service teachers at one of the public universities. The study concluded that the level of awareness of pre-service teachers from the study sample about digital data security, cyber bullying and digital ethics was high, and it showed no differences according to academic level in the level of awareness, but it confirmed the presence of statistically significant differences in the level of awareness according to gender and specialization.

(Samara, 2023) showed that Cybersecurity is one of the most important elements of security in developed countries. Especially since there is an overall trend towards cybersecurity

in all aspects of life, the study found that the idea of cybersecurity is based on protecting critical facilities: The nation's information infrastructure, information systems, including e-government management systems, are managed by key state agencies. As with economic, scientific, commercial, and other systems, there are threats to a nation's national security. The study showed that they found many countries are preparing institutions capable of integrating cybersecurity into protection, development, and information security. This concept has become the most important concern of developed countries, which have secured all scientific possibilities and systems to achieve it. The study showed that the electronic information network has become an integral part of today's daily lives in all places, in addition to personal uses, digital information is used, processed, stored and shared. The study found that the protection has become more vital and has an effective impact on national security and technical progress.

(Saeed, 2023) followed the systematic literature review explores the digital transformation (DT) and cybersecurity implications for achieving business resilience. DT involves transitioning organizational processes to it solutions, which can result in significant changes across various aspects of an organization. However, emerging technologies such as artificial intelligence, big data and analytics, block chain, cloud computing drive digital transformation worldwide while increasing cybersecurity risks for businesses undergoing this process. This literature survey article highlights that the importance of comprehensive knowledge of cybersecurity threats during DT implementation to prevent interruptions due to malicious activities or unauthorized access by attackers aiming at sensitive information alteration, destruction, or extortion from users. Cybersecurity was essential to DT as it protects digital assets from cyber threats. This study conducted a systematic literature review using the PRISMA methodology in this research. This literature review found that DT has increased efficiency and productivity but poses new challenges related to cybersecurity risks, such as data breaches and cyber-attacks. The study concluded by discussing future vulnerabilities associated with DT implementation and provide recommendations on how organizations can mitigate these risks through effective cybersecurity measures. This study recommended a staged cybersecurity readiness framework for business organizations to be prepared to pursue digital transformation.

(Bhukya, et al., 2023) showed that the "Internet-of-Medical-Vehicles (IOMV)" is one of the special applications of the Internet of things resulting from combining connected healthcare and connected vehicles, as the IOMV communicates with a variety of networks along its travel path, it incurs various security risks due to sophisticated cyber-attacks. This study can endanger the onboard patient's life. So, it is critical to understand subjects related to "cyber security" in the IOMV to develop robust cybersecurity measures. In this paper, the goal is to evaluate recent trends and state-of-the-art publications, gaps, and future outlooks related to this study area. With this aim, a variety of publications between 2016 and 2023 from "Web-of-Science" and "Scopus" databases were analyzed. The analysis of this study revealed that the IOMV is a niche and unexplored research area with few defined standards and frameworks, and there is a great need to implement robust cybersecurity measures. This study will help researchers to gain a comprehensive idea of this niche research topic, as it presents an analysis of top journals and highly cited papers, their challenges and limitations, the system model and architecture of the IOMV, related applicable standards, potential cyber-attacks, factors causing cybersecurity risks, various artificial intelligence techniques for developing potential countermeasures, the assessment and parameterization of cybersecurity risks, constraints and challenges, and future outlooks for implementing cybersecurity measures in the IOMV.

(Admass, 2024) discussed the prevailing values and provides an overview of the state of the art in cyber security, challenges, and tactics, current conditions, and global trends of

cyber security. The study showed that to stay ahead of the curve in cyber security, they conducted a systematic review to uncover the latest trends, challenges, and state-of-the-art in cyber security. Moreover, they address the future direction of cyber security, presenting the possible strategies and approaches to addressing the increasing cybersecurity threat landscapes, the emerging trends, and innovations like Artificial Intelligence (AI) and machine learning (ML) to detect and automate cyber threat responses. This study underlines the importance of ongoing adoption along with collaboration among stakeholders in the cyber ecosystem.

(Binnar, et al., 2024) showed that there is a great demand for an efficient security tool which can secure IIoT systems from potential adversarial attacks. However, it is challenging to design a suitable security model for IIoT considering the closed, dynamic and distributed architecture. This motivates the researchers to focus more on investigating the role of forensic tools such as DFIR in the designing of security models. This study showed that a brief analysis of the security issues, challenges and attacks on IIoT systems is presented in this paper with an emphasis of DFIR for the security of ICS, CPS, and SCADA. The security recommendations for IIoT, forensic challenges in SCADA, ICS and CPS are discussed. The study suggested that forensic tools can overcome the drawbacks of conventional security solutions in terms of maintaining the privacy of data while sharing information with other systems. This study discussed a different models, overview, comparisons, and summarization of DFIR and intrusion detection systems (IDS)-based techniques for IIoT security. In addition, this review analyzes the challenges and research gaps based on the existing literary works.

Comment on previous studies:

By reviewing previous studies, the following was revealed:

First: The differences between the current study and previous studies:

- In terms of study variables: The current study differed from previous studies, as no study was found that addressed the variable of the level of awareness of faculty members at the University of Hail about cybersecurity requirements.
- In terms of the study sample: The current study differed from previous studies in terms of the target group. The current study targeted faculty members at the University of Hail, while (Al-Habib, 2022) dealt with graduate students in colleges of education, and the study by (Zaqout et al., 2022) dealt with faculty members at Zawia University.

Second: Benefits from previous studies:
By reviewing previous studies, they were used to build the theoretical framework of the study, build the current study tool, and choose the appropriate statistical treatment method with the study variables.

Third: Areas of agreement between the current study and previous studies:

In terms of the study method: The current study agreed with many previous studies in the study method used, which is the descriptive method, including the study of (Dawson et al. ,2022; Al-Habib, 2022 ;Tawfiq and Morsi, 2023).

In terms of objectives: The current study agreed with many studies that aimed to study the level of faculty members' awareness of cybersecurity requirements: the study of (Zaqout et al., 2022 ; Tawfiq and Morsi, 2023)

In terms of tools: The current study agreed with many studies in study tools, as it relied on the questionnaire, including (Al-Aqla and Ali, 2022 ; Farag, 2022 ; Al-Manea ,2022).

Study procedures:

Research community:
The research community includes all faculty members at the University of Hail.

Study Sample:
The study sample consists of a random group of faculty members at the University of Hail, and their total number reached (343), distributed among health colleges, scientific colleges, humanities colleges, and the applied college.

Description of the Study Sample:
The following table shows the distribution of the study sample according to the demographic variables of the study:

Table (1): Distribution of the study sample according to demographic variables

variable	Category	Frequency	%
Colleges	Health colleges	91	%26.5
	Scientific colleges	84	%24.5
	Humanities colleges	119	%34.7
	Applied colleges	49	%14.3
Scientific degree	lecturer	14	%4.1
	Assistant Professor	245	%71.4
	Associate Professor	56	%16.3
	Professor	28	%8.2
Years of Experience	Less than 5 years	49	%14.3
	From 6-10 years	84	%24.5
	More than 10 years	210	%61.2

Source: Collected and calculated from the analysis of the study sample by using SPSS.

1-The study tool and its construction procedures:
The questionnaire was used to answer the study's questions, which were to determine the requirements for achieving cybersecurity at the University of Hail, and to identify the obstacles to activating cybersecurity requirements from the viewpoint of university faculty members. To prepare the questionnaire, previous literature and studies related to the subject of the study were reviewed and used as guidance in determining the questionnaire's axes and items. The initial version of the questionnaire was reached, and to ensure the validity and reliability of the questionnaire by the following:

Adjust the resolution scientifically: This is done by calculating the validity and reliability coefficients as follows:

Honesty of arbitrators: To ensure the logical validity of the questionnaire, it was presented to a group of arbitrators specialized in the field of cybersecurity and information technology. To get their opinions and suggestions in the questionnaire, their opinions and suggestions included the stability of the questionnaire for the purpose for which it was prepared, the stability and clarity of its instructions, the reformulation of some vocabulary and the modification of others, and the reformulation of some difficult and ambiguous sentences and words for some of the questionnaire vocabulary. The necessary amendments were made to the questionnaire in light of the opinions of the arbitrators.

Calculating the Stability Coefficient:

The reliability coefficient of the questionnaire was calculated using the method of calculating the variance of the questionnaire items, by applying it once to the sample of the exploratory study, which numbered (12) faculty members at the University of Hail. Then the results were monitored and processed using the (Cronbach's alpha) equation to calculate the reliability coefficient of the questionnaire. The split-half method was used to calculate the reliability coefficient to ensure the reliability of the questionnaire as a whole. The table (2) shows this.

Table (2): Reliability coefficient of the questionnaire

Number of phrases	Correlation with half split	Cronbach's alpha coefficient
343	0.881	0.867

Source: Calculated from the analysis of the study sample by using SPSS.

It is clear from the table (2), the reliability coefficient of the questionnaire as a whole using Cronbach's alpha was about (0.867) and using split-half was about (0.881), which was a high reliability coefficient.

Correction the Questionnaire:

The following method was used to determine the level of response to the questionnaire items, where weight was given to the alternatives shown in the following table in order to be treated statistically as follows:

Table (3): Correcting the questionnaire

Strongly Disagree	Disagree	Neutral	OK	Strongly Agree	Response
1	2	3	4	5	Degree

Source: Calculated from the analysis of the study sample by using SPSS.

These responses were then classified into five equal levels to obtain the following classification:

Table (4): Distribution of categories according to the hierarchy

Range of averages	Description
From 4.21 -5.00	Strongly Agree
From 3.41- 4.20	Agree
From 2.61- 3.40	Neutral
From 1.81-2.60	Disagree
1.80 -1.00من	Strongly Disagree

Source: Calculated from the analysis of the study sample by using SPSS.

Analyzed and discussed the results:

First, the requirements for achieving cybersecurity at the University of Hail:

To determine the requirements for achieving cybersecurity at the University of Hail from the viewpoint of the university's faculty members, the ranking, rating score, mean, and standard deviation of the questionnaire's axes were calculated as follows:

Table (5): Average requirements for achieving cybersecurity at the University of Hail from the viewpoint of university faculty members

	Cybersecurity Requirements	Average	St. deviation	Ranking	Description

1	the first axis: Technical Requirements	4.26	0.931	2	Strongly Agree
2	the second axis: Physical Requirements	4.21	0.788	3	Strongly Agree
3	the third axis: Human Requirements	4.33	0.833	1	Strongly Agree
4	fourth axis: Cognitive Requirements	3.76	0.944	5	Agree
5	fifth axis: Administrative Requirements	3.82	1.167	4	Agree
Total		**4.07**	**0.933**		

Source: Calculated from the analysis of the study sample by using SPSS.

It is clear from the previous table that the requirements for achieving cybersecurity at the University of Hail were rated appropriately from the point of view of the faculty members, that the mean for cybersecurity requirements reached about (4.07) , the standard deviation reached about (0.933). The Human requirements came in the first place with a mean reached about (4.33) with a rating of strongly agree from the viewpoint of the faculty members at the University of Hail. This confirmed the importance of human requirements in achieving cybersecurity requirements and that they have a fundamental role in that. The results showed that the Cybersecurity requirements cannot be achieved without the availability of a qualified human element. So, In the second ranking for the requirements for achieving cybersecurity at the University of Hail, the technical requirements came with an average reached about (4.26), the third ranking came the physical requirements with an average of about (4.21), both with a rating that strongly agree with the viewpoint of the faculty members at the University of Hail. In the fourth ranking the administrative requirements came with an average reached about (3.82). The final ranking of cognitive requirements came with an average reached about (3.76), both with a rating that agree only with the viewpoint of the faculty members at the University of Hail.

Second: Obstacles to achieving cybersecurity at the University of Hail:

Table (6): Results of the obstacles of achieving cybersecurity at the University of Hail from the viewpoint of the university's faculty members

	Cybersecurity requirements	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Mean	St. deviation	Ranking	Degree of Agree
1	The lack of an approved strategy to achieve cybersecurity at the University of Hail	119	70	63	42	49	4.18	0.858	2	Agree
2	Lack of adequate protection systems against modern hacking programs	34.7	20.4	18.4	12.2	14.3			10	Agree

3	The low level of experience of faculty members at Hail University with cybersecurity requirements.	112	98	42	42	49	3.49	1.445	9	Agree
4	Weak application of cybersecurity governance standards at the University of Hail	32.7	28.6	12.2	12.2	14.3			1	Strongly Agree
5	There are no guarantees for implementing cybersecurity policies at the University of Hail	203	63	63	14	0	3.53	1.430	8	Agree
6	Weak technical standards that support cybersecurity procedures at the University of Hail	59.2	18.4	18.4	4.1	0.0			14	Neutral
7	There is no accredited cybersecurity risk management affiliated with the Cybersecurity Department at the University of Hail	91	84	119	21	28	4.33	0.922	7	Agree
8	There is no periodic cybersecurity risk assessment at the University of Hail	26.5	24.5	34.7	6.1	8.2			5	Agree
9	Not conducting a security	35	84	91	77	56	3.55	1.191	4	Agree

	survey for workers in cybersecurity positions at the university									
10	Lack of protection programs against viruses and suspicious activity programs on electronic devices at the university	10.2	24.5	26.5	22.4	16.3			6	Agree
11	Lack of electronic archive and backup copies of electronic data for faculty members and students	98	119	70	21	35	2.90	1.246	3	Agree
12	There are no secure coding standards for application development at the University of Hail	28.6	34.7	20.4	6.1	10.2			13	Agree
13	The contracts of university employees do not include a special clause clarifying cybersecurity responsibilities and clauses for maintaining the confidentiality of information	119	105	77	21	21	3.65	1.251	11	Agree
14	Weak cybersecurity awareness programs targeting faculty and students.	34.7	30.6	22.4	6.1	6.1			12	Agree

15	There is no accreditation for cybersecurity requirements for the security of mobile devices and personal devices of university employees	140	70	84	49	0	3.82	1.167	9	Agree
	Total	3.66						1.177	Agree	

Source: Calculated from the analysis of the study sample by using SPSS.

To determine the obstacles of achieving cybersecurity at the University of Hail from the viewpoint of the university's faculty members, the frequency, percentage, ranking, rating score, mean, and standard deviation of the axis phrases were calculated from table (6).

It is clear from the table (6) that the challenges facing the fulfillment of cybersecurity requirements at the University of Hail from the point of view of faculty members were rated agree, as the overall mean for cybersecurity requirements reached about (3.66) and a standard deviation reached about (1.177), this confirmed the high level of challenges faced by members the faculty at the University of Hail prevents the employment of cybersecurity requirements at the University of Hail, which requires studying those challenges and providing solutions and suggestions to overcome those challenges. The challenge "Weak application of cybersecurity governance standards at the University of Hail" came in first place with mean about (4.33) with a rating that strongly agrees with the viewpoint of faculty members at the University of Hail. The challenge "The lack of an approved strategy to achieve cybersecurity at the University of Hail" came in second place, and this confirmed that the importance and necessity of the University of Hail adopting declared, documented and approved standards by the university director for cybersecurity governance, and developing an approved strategy to achieve cybersecurity requirements at the University of Hail; Standards and strategy were the first step to effectively achieving cybersecurity requirements.

Study Recommendations:

1- Needing for the University of Hail to pay attention to developing an approved strategy to achieve the university's cybersecurity requirements.
2- The University of Hail should work to adopt standards for cybersecurity governance that will be announced to all university employees.
3- The Cybersecurity Department at the University of Hail works to provide various awareness programs on cybersecurity targeting all university employees and students.
4- The University of Hail should adopt a specific mechanism for periodic follow-up and evaluation of the university's cybersecurity requirements.
5- Encouraging faculty members to conduct more research on cyber security, its requirements, and mechanisms for activating it.

Acknowledgements: The author acknowledge support for the underlying study into requirements and challenges of achieving cybersecurity from the point of view Faculty

members at the University of Hail from a Faculty of Education and Information Technology, Computer Science and Engineering, University of Hail, Saudi Arab Kingdom.

References:

Admass W.S., et al., (2024): Cyber security: State of the art, challenges and future directions, Cybersecurity and Applications, Volume 2. https://doi.org/10.1016/j.csa.2023.100031

Al-Alfi, M.(2010): Some methods of combating crime on information systems in organizations: Online crime control seminars held at the Administrative Development Organization, "Protection Information and Electronic Signature" workshop, Cairo: Administrative Development Organization, 83:100. https://search.mandumah.com/Record/125053

Al-Aqlaa, R.A., Ali, A.N.(2022): The degree of awareness of cybersecurity concepts among computer teachers in Hail. Arab Studies in Education and Psychology, 144(2), 279: 300. https://doi.org/10.21608/saep.2022.263396

Al-Bishi, M.A.(2021): Cybersecurity in Saudi universities and its impact on enhancing digital trust from the point of view of faculty members: A study on Bisha University. Islamic University Journal for Educational and Psychological Studies, 29(6), 353:372. https://journals.ekb.eg/article_222076.html#:~:text=DOI%3A%2010.12816/mfes.2022.222076

Al-Habib, M.A.(2022): The degree of awareness of cybersecurity among male and female postgraduate students at the College of Education at Imam Muhammad bin Saud Islamic University and ways to enhance it from their point of view, Journal of Educational Sciences. 30, 326: 269. https://imamjournals.org/index.php/joes/article/view/2085

Al-Haddad, N.M. (2022): Requirements for achieving cybersecurity in Yemeni university libraries: A case study. Al Bayda University Journal 4(2), 703: 716. https://doi.org/10.56807/buj.v4i2.287

Al-Jundi, A.A., Mohammad, N.T.(2019): The role of applied cybersecurity practice in developing skills and accuracy of practical application of information security among female university students, World of Education Magazine - Arab Foundation for Scientific Consultation and Human Resources Development. 67(3), 14: 84. https://search.mandumah.com/Record/1109673

Al-Manea, A.A.(2022): Requirements for achieving cybersecurity in Saudi universities in light of Vision 2020, Journal of the College of Education (Assiut), 38 (1), 155: 194. https://mfes.journals.ekb.eg/article_222076.html

Al-Montashari, F.Y. (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, Arab Foundation for Education, Science and Arts. 17, 384: 357. https://jasep.journals.ekb.eg/article_100703.html#:~:text=10.33850/JASEP.2020.100703

Al-Montashari, F.Y., Hariri, R.(2020): The degree of middle school teachers' awareness of cybersecurity in public schools in Jeddah from the teachers' point of view, Arab Journal of Specific Education, 4(14), 95: 140. https://ejev.journals.ekb.eg/article_101830.html#:~:text=10.33850/EJEV.2020.101830

Al-Mutairi, M.S. (2021): The reality of cybersecurity and increasing its effectiveness in public education schools in the Medina region from the point of view of school leadership. International Journal of Educational and Psychological Studies, 10(3), 635: 655. http://dx.doi.org/10.31559/EPS2021.10.3.7

Al-Qahtani, N.b.N. (2019): The extent of awareness of cybersecurity among male and female students at Saudi universities from a social perspective: a field study, Social Affairs Magazine - Sharjah Socialists Association, 36(144), 85: 120. https://search.emarefa.net/ar/detail/BIM-922380-%D9%85%D8%AF%D9%89-%D8%AA%D9%88%D9%81%D8%B1-D8%A7%D9%84%D9%88%D8%B9%D9%8A-%D8%A8%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D9%84%D8%AF%D9%89-%D8%B7%D9%84%D8%A7%D8%A8-%D9%88-%D8%B7%D8%A7%D9%84%D8%A8%D8%A7%D8%AA-%D8%A7%D9%84%D8%AC%D8%A7%D9%85%D8%B9%D8%A7%D8%AA-%D8%A7

Al-Rukban, A.O. (2023): Achieving cybersecurity for management information systems at Imam Muhammad bin Saud Islamic University: An evaluation study, Arab Journal for Educational and Social Studies, (20).

https://ae.linkedin.com/pulse/%D8%AA%D9%82%D8%B1%D9%8A%D8%B1-%D8%A7%D8%B3%D8%AA%D8%B7%D9%84%D8%A7%D8%B9-%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D9%84%D8%B9%D8%A7%D9%85-2023-%D8%A7%D9%84%D9%86%D9%85%D9%88-%D8%A7%D9%84%D9%85%D8%AA%D8%B2%D8%A7%D9%8A%D8%AF

Al-Sahafy, M.A., Askoul, S.S. (2019): The level of cybersecurity awareness among secondary school computer teachers in Jeddah, Journal of Scientific Research in Education, 20(10), 493:534. https://search.mandumah.com/Record/1029923

Al-Samhan, M.A. (2020): Requirements for achieving cybersecurity for management information systems at King Saud University: An evaluation study, Journal of the Faculty of Education, Mansoura University, (111) 3: 28. https://doi.org/10.21608/maed.2010.140786

Al-Sanea, N.O.(2020): Teachers' awareness of cybersecurity and ways to protect students from Internet risks and enhance their national values and identity, College of Education Journal, 36(6), 41:90. https://search.mandumah.com/Record/1085483

Al-Timani, M.Z., Abdul, R. (2021): The reality of information awareness of cybersecurity among individuals in Saudi society, as perceived by cybersecurity experts. Journal of Social Work, 67, 1:23. https://doi.org/10.21608/egjsw.2021.170843

Bhukya, et al., (2023) Cybersecurity in Internet of Medical Vehicles: State-of-the-Art Analysis, Research Challenges and Future Perspectives, Sensors (Basel). Oct; 23(19): 8107. https://doi.org/10.3390%2Fs23198107

Binnar, P., et al., (2024): Security analysis of cyber physical system using digital forensic incident response, Cybersecurity and Applications, Volume 2, 100034. https://doi.org/10.1016/j.csa.2023.100034

Dawson, K., et al. (2022): Promoting Interdisciplinary integration of cybersecurity Knowledge, Skills, and career Awareness in Preservice Teacher Education, Association for the Advancement of Computing in Education, 30(2), 275. https://ialt.education.ufl.edu/wp-content/uploads/sites/8/2022/08/Promoting-Interdisciplinary-Integration-of-Cybersecurity-Knowledge-Skills-and-Career-Awareness-in-Preservice-Teacher-Education.pdf

Faraj, A.O. (2022): Reasons for promoting a culture of cybersecurity in light of digital transformation - Prince Sattam bin Abdulaziz University as a model. Educational Journal of the Faculty of Education in Sohag, 94(94), 509-537. https://doi.org/10.21608/edusohag.2022.212365

Gümüş, M.M., Çakır, R.K. (2023): Investigation of pre-service teachers' sensitivity to cyberbullying, perceptions of digital ethics and awareness of digital data security, Education and Information Technologies, 63.1-23. https://link.springer.com/article/10.1007/s10639-023-11785-7

Hong, W.C. , et al. (2023): The Influence of Social Education Level on Cybersecurity Awareness and Behaviour: A Comparative Study of University Students and Working Graduates, Education and Information Technologies, 28 (1), 439:470. https://link.springer.com/article/10.1007/s10639-022-11121-5

Human Resources Development Fund (2021): Annual Report. https://www.hrdf.org.sa/annualreports

Kaoua, A.A.(2020): Cybersecurity policies to enhance digital transformation in Egyptian universities: A proposed vision in light of global experiences, Educational and Social Studies, 26(3), 133: 200. https://doi.org/10.21608/jsu.2020.231281

Kingdom's Vision, 2023. https://www.moh.gov.sa/Ministry/About/Strategy_Policies_SLA/Pages/Digital-Transformation.aspx

Mihci, T.P.,Kiliç, Ç.E.(2019): An Investigation of Cyber Wellness Awareness: Turkey Secondary School Students, Teachers, and Parents, Computers in the Schools, 36 (4), 293:318. https://eric.ed.gov/?id=EJ1236066

Ministry of Education, National Cybersecurity Authority (2021): Cooperation agreement between the Ministry of Education and the National Cybersecurity Authority in the fields of scientific research and qualification of national cadres. Riyadh: The Ministry's Media Center. https://www.moe.gov.sa/ar/mediacenter/MOEnews/Pages/am1442-876.aspx

National Committee for Digital Transformation (2020): Annual National Digital Transformation Report for 2020. Riyadh: Authority's Media Center. https://www.vision2030.gov.sa/media/yg0fggps/annual-ntp-report-2022-ar.pdf

National Cybersecurity Authority, (2018): Basic cybersecurity controls, Riyadh National Cybersecurity Authority. https://ega.ee/wp-content/uploads/2019/03/Essential-Cybersecurity-Controls.pdf

National Guidance Centre for Cybersecurity (2023): Security Awareness. https://cert.gov.sa/ar

Richardson, M., et al., (2020): Planning for cybersecurity in school: the human factor, Educational planning, 27(2), 23: 39. https://eric.ed.gov/?id=EJ1252710

Riley, S (2022): Independent School Districts in Texas: A Focused Ethnography on Cybersecurity Barriers, ProQuest LLC, D.B.A. Dissertation, North central University. https://eric.ed.gov/?id=ED620030

Saeed, S., et al., (2023): Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations, Sensors (Basel). Aug; 23(15). https://doi.org/10.3390%2Fs23156666

Samara, N.K. (2023): Cybersecurity Requirements for Management Information Systems, Journal of Information Security, Vol.14 No.3, July. https://doi.org/10.4236/jis.2023.143013

Tawfiq, S. A. , Morsi, S.E.(2023):Requirements for achieving cybersecurity in Egyptian universities in light of digital transformation from the point of view of faculty members (Benha University as an example), Educational Journal of the Faculty of Education at Sohag University, 105(105), 737: 866. https://doi.org/10.21608/edusohag.2023.283004

Zaqut, N. I., et al., (2022): The extent of awareness of faculty members in Libyan universities of the importance of cybersecurity in light of digital transformation - an applied study at Zawia University. International Journal of Science and Technology, 22(1), 1:22. https://www.stcrs.com.ly/istj/article-details.php?id=481