International Journal of Academic Information Systems Research (IJAISR)
ISSN: 2643-9026
Vol. 6 Issue 11, November - 2022, Pages: 29-43

The Extent of Cyber Security Application at the Ministry Of Interior and National Security in Palestine

Mahmoud T. Al Najjar[1], Mazen J. Al Shobaki[2], Suliman A. El Talla[3]

[1]Faculty of Administrative and Financial Sciences, Israa University – Gaza, Palestine.
[3]College of Intermediate Studies – Al-Azhar University – Gaza, Palestin
[1]malekzain750@gmail.com, [2]mazen.alshobaki@gmail.com, [3]Eltallasuliman@gmail.com

Abstract: *This study aimed to identify the extent of the application of Cyber Security at the Ministry of Interior and National Security from the point of view of workers in the computer and information technology units. 70 employees, and the study tool (questionnaire) was distributed, and the comprehensive survey method was used, as (61) questionnaires were retrieved at a rate of (87.1%), and they were unloaded and analyzed using the SPSS statistical package.The study reached several results, including: There was a high degree of agreement on the degree of Cyber Security application, which amounted to (74.8%). With a relative weight of (74.8%), and The Dimension efforts to monitor threats, it received a high degree of approval and a relative weight of (73.4%). Privacy has a high degree of approval with a relative weight of (78.4%).The study presented a set of recommendations, the most important of which are: the need to pay attention to providing the Ministry of Interior and National Security with a budget in order to activate and improve the Cyber Security system, and the need for the Ministry of Interior and National Security to use a protection network capable of detecting all threats, and the cooperation of the Ministry of Interior and National Security with external institutions to limit penetration of network systems, In addition to the need to continuously strengthen and develop the laws and legislations of the Ministry of Interior in line with the development of Cyber Security, and to enhance the capabilities of the public beneficiaries of the ministry's electronic services to reduce security gaps in the field of Cyber Security.*

Keywords: Cyber Security, Ministry of Interior and National Security, Gaza Strip, Palestine.

Introduction

The technological progress and the information revolution that the world has witnessed in the world of communications for decades have brought about tremendous changes and a positive impact on the business world through the introduction of new variables. Raising efficiency in addition to improving performance levels based on harnessing the capabilities of this technology on the human element, which represents the main driver for the use of these technologies. It is not necessary to abolish all traditional systems.

According to the study (Bahour, 2016), the benefit of these advanced technologies in the public and private sector institutions operating in Gaza Strip still does not rise to the desired level due to the presence of some challenges, especially in the field of readiness of these organizations to manage and implement such modern concepts, and among these challenges is the spread of The phenomenon of cybercrime and the penetration of information centers, which prompted decision makers in organizations to seriously think about following methods and procedures to confront these crimes, and the use of safe systems known as the Cyber Security Department and it is interested in providing advanced systems and protocols in order to protect data from these risks, taking into account the need to monitor Threats and evaluate them first, as cyber security is a strategic weapon to confront these risks.

The researchers believe that the Cyber Security Department helps organizations, including the Ministry of Interior, to provide electronic services at low costs, in addition to growing their work, obtaining good statistics and data analysis, and helping them to face some challenges represented in the dangers of cybercrime.

Based on the foregoing, the study seeks to highlight the extent of the application of Cyber Security in the Ministry of Interior and National Security in Gaza Strip, and the importance of Cyber Security in facing the challenges that may hinder the work of the ministry will be addressed from the point of view of computer and information technology units.

Definition of Key Terms

There are many terms that were used in the study, the most important of which are:

- **Cyber Security**: A set of technical and administrative measures that include the processes and mechanisms applied by institutions to secure their digital infrastructure and maintain the confidentiality of data and information (Al-Jifnawi, 2021).
- **Procedural Definition**: A set of technical, organizational and administrative means adopted by organizations that are used to prevent network penetration and maintain digital infrastructure.
- **The Ministry of Interior and National Security**: It is one of the sovereign and most important ministries in the Palestinian government, as it performs an outstanding performance in carrying out its tasks and ensuring the interest of the homeland and the citizen, organizing civil life, and implementing the law for everyone (http://www.moi.gov.ps).

Problem Statement

Although governmental institutions in Gaza Strip, including the Ministry of Interior, have many scientific and practical achievements, they still face many challenges and obstacles, the most prominent of which are electronic hacking operations and attempts to steal data. From this standpoint, it has become necessary for all organizations to adopt a number of approaches. Which contribute to the provision of rules and systems of protection in order to address electronic penetration and this is one of the most important tasks of the Department of Cyber Security, so this study comes to shed light on the importance of Cyber Security and the availability of the necessary requirements for the Department of Security to be adopted in administrative work, and to provide services to the public taking into account the security and privacy of data.

Based on the foregoing, it appeared to the researchers the problem of the study and its importance, so the study will focus on exploring the extent of the application of Cyber Security in the Ministry of Interior and National Security - Gaza Strip.

Research Questions

From the foregoing, the main question that the head will answer has been concluded, which is:

What is the reality of applying the requirements of Cyber Security by the Ministry of Interior and National Security from the point of view of workers in computer and information technology units?

A number of sub-questions will be divided, which the study will answer, as follows:

Q1-: What is the availability of organizational efforts in the Ministry of Interior necessary to manage cyber security?

Q2-: What is the availability of technical efforts in the Ministry of Interior necessary to manage cyber security?

Q3-: What is the availability of threat monitoring efforts in the Ministry of Interior necessary to manage cyber security?

Q4-: What is the availability of laws and legislations in the Ministry of Interior and National Security necessary for cyber security?

Q5-: How appropriate is Privacy Protection for the Cyber Security Department of the Department of Homeland Security and Homeland Security?

Q6-: What are the most important challenges facing the Ministry of Interior and National Security to manage Cyber Security?

Research Objectives

Based on the established research questions, this study aims to achieve the following objectives:

1. Knowing the reality of applying cyber security at the Ministry of Interior and National Security.
2. Identify the most important challenges facing Cyber Security management.
3. Coming up with recommendations that contribute to enhancing the implementation and management of Cyber Security.

Research Importance

The aspects of the importance of the study can be identified from the contribution and the expected addition from it, as follows:

Scientific (Theoretical) Importance:

1. The importance of this scientific study is evident in the fact that the application of cybersecurity is one of the most important modern technologies that help in preserving data and preventing penetration, which helps in improving the performance of institutions in terms of quality and improving the service provided by these institutions to beneficiaries, for its role in providing distinguished programs and applications, monitoring and saving data in a safe and less Cost.
2. Enriching scientific research on this topic, as it is considered one of the modern topics, according to the researchers' point of view.

Practical (Applied) Importance:

1. Works to support decision-making at the Ministry.
2. May support the oversight process of the Ministry's services and projects.
3. Assist in organizing and arranging work within the ministry.

Research Limits and Scope

The scope of the study shall be as follows:

1. **Objective Limits**: The study focused on the extent to which Cyber Security is applied.
2. **Human Limits**: The study was conducted on workers in the computer and information technology units of the Ministry of Interior.
3. **Institutional Limits**: The study was conducted on a sample of workers in the Ministry of Interior - the southern governorates.
4. **Spatial Limits**: The study was conducted in the State of Palestine, Gaza Strip.
5. **Temporal Limits**: the year 2022.

Previous Studies

- A study of (Al-Jifnawi, 2021) titled "Digital Transformation of National Institutions and Cyber Security Challenges from the Point of View of Academic Police Officers in Kuwait", which aimed to identify the digital transformation and challenges of Cyber Security in the State of Kuwait from the point of view of academic officers, and the researcher used the descriptive analytical approach To achieve the objectives of the study, and to collect data for the study, the researcher designed a questionnaire and distributed it to the study sample consisting of 80 academic officers. For educational qualification, experience, age and training courses.
- A study of (Faraj, 2021), which aimed to address the reasons and importance of promoting a culture of Cyber Security in light of Prince Sattam University’s adoption of digital transformation according to a number of variables, the most important of which are the years of experience in addition to the scientific specialization. Purpose The researcher built a questionnaire consisting of

26 paragraphs, and it was distributed to the study sample, which amounted to 125 members of the faculty at the university. This was followed by the cognitive reasoning axis, and finally the technical reasoning axis.

- A study of (Moskal, 2020), which aimed to study the importance of enhancing Cyber Security in American universities in light of the digital transformation, and the researcher used the descriptive approach to achieve the purpose of the study, and the researcher built a special questionnaire to collect data from the study sample of 100 American universities, and the study showed the importance of developing a vision To establish a cyber security center in American universities with the aim of increasing cyber awareness.
- A study of (Al-Sanea et al., 2020), which aimed to identify the degree of awareness of teachers about Cyber Security and its relationship to national values. The study raises teachers' awareness of cyber security in the field of protecting private devices.
- A study of (Al-Qahtani, 2019), which aimed to identify the extent of awareness of Cyber Security among university students in Saudi universities, in addition to studying the most important methods of community prevention from cybercrime. The researcher used the analytical descriptive approach, and the researcher built a special questionnaire to collect data Of the study sample, which amounted to 486 male and female students, the study showed that the crime of electronic fraud is the most common crime that Cyber Security deals with.
- A study of (Al-Jundi, 2019), which aimed to identify the importance of practicing and applying Cyber Security and the accuracy of the practical application of information security. The researcher used the descriptive analytical approach to achieve the objectives of the study. The researcher collected data through a special questionnaire that was distributed to the study sample, which amounted to 80 students. From the Department of Computer Science at Umm Al-Qura University. The study showed that the application of Cyber Security practices will enable students to understand the guiding standards for conducting risk assessments.
- A study of (Catota & Sicker, 2019) aimed at clarifying the importance of building national capacities for Cyber Security, which were relied upon to successfully confront cyberattacks, in addition to the importance of drawing up a national strategy for Cyber Security through which you can protect the digital technological infrastructure of developing countries. Cyber programs and technological awareness, in addition to cooperation and integration of roles between universities contribute to the promotion of cyber culture.
- A study of (Maranga & Nelson, 2019), which aimed to identify ways universities secure their sites and data from cyber-attacks, and to achieve the purpose of the study, the researchers used the descriptive analytical approach through the questionnaire as a tool for collecting data from university workers. The study showed that one of the most important means of protecting universities is good planning of mechanisms Cyber security, in addition to spreading cyber concepts.
- A study of (Al-Arishi and Al-Dosari, 2018), which aimed to study the electronic risks that threaten information security in cyberspace, and the study also touched on the most important procedures that must be followed to promote a culture of Cyber Security in society. The researcher built a special questionnaire to collect data that contributes to achieving the objectives of the study, while the study sample consisted of 702 students from King Saud University. The study showed that the development of cultural thought on the importance of information security is one of the most important roles of society to promote a culture of Cyber Security.
- A study of (Ninkeu, 2018), which aimed the study to identify the concepts of cyber security and cyber violations, and to achieve the purpose of the study, the researcher used the interview as a tool to collect data from the study sample, who are the students of the Catholic University, and the study showed that there is a weakness among university students in the concepts of internet security and cyber security in addition to cyber risks, and the study recommended the need to strengthen cyber security concepts by including them in academic curricula.

Commenting On Previous Studies

It is clear from a review of previous studies that these studies have varied and differed according to the goals they sought to achieve, as well as the different environments in which they were applied, the variables they studied, the methods used and the tools that were used. Below, the researchers will present the most important aspects of agreement and disagreement, as well as what distinguishes his study about previous studies:

Advantages of previous studies

- Enriching the theoretical framework in the study.
- Building the questionnaire study tool.
- Ensure that the current study is not repeated.
- Provide the necessary references for the study, especially foreign references.

The Study Is Characterized

- The study was applied to the environment of government sector institutions in Gaza Strip, and as far as the researchers are aware, this is the first study that studies the management of the Ministry of Interior and National Security for the process of applying cyber security.

- Using a number of tools for data, as the researchers relied on more than one method in collecting primary data, most notably interviews, questionnaires, and holding a workshop.

Theoretical Framework

Cyber security includes protecting the privacy of data and key devices from external risks and cyber threats. According to (Al-Jifnawi, 2021), the origin of the word cyber security goes back to the Latin word Cyber, by which we mean information space, and by this cyber security we mean the security of information space. (Al-Bahi, 2017) said that Cyber Security is linked to the World Wide Web and the communications network, where Cyber Security represents the basic pillar of any digital transformation, and according to (Al-Janabi, 2017), Cyber Security aims directly at moving from routine work to technical work in its various forms through The use of non-traditional techniques, and the most important of these technologies is computer networks that depend on linking all organizational units with each other, in addition to the oversight bodies charged with following up the workflow, preserving information accurately, and facilitating dealing with it with better accuracy, in addition to the main role of the oversight bodies represented in Identify hackers' devices and their identity.

Kennedy (2017) was defined as a system that works to protect electronic data from risks through the use of organizations for a group of technical and administrative means in order to protect the privacy of data and files, in addition to taking the necessary measures to protect them.

(Qari et al And their data from the electronic attacks that target them, and it is measured by the degree that the teacher gets through his answer to the cybersecurity paragraphs, and he (Al-ManThari, 2020) is known as a security concept for the protection of information and all its money is related to that information of operations, services and technologies against any external danger, or Use it negatively.

(Richardson Etc Al, 2020) is known as the technical security and precautions that are followed for the garrison of devices, information systems and data from unauthorized access to maintain the safety and integrity of the data stored in digital devices.

The researchers adopt a procedural definition of cybersecurity as a set of technical, organizational and administrative means that are used to institutions that are used to prevent networking and maintaining digital infrastructure.

Cyber Security Departments:

Moore (2018) divided Cyber Security into several sections, namely:

- Communications Security: It aims to protect against threats affecting the infrastructure and technology of communications and to protect and preserve it from any external threat.
- Operations security: It aims to protect operations and workflow methods from any external risks.
- Information security: It aims to protect information and restrict access to it by unauthorized persons, in addition to protecting its privacy from theft.
- Physical security: It aims to protect the physical assets related to the cyber system, such as servers and electronic networks, from any external risks.
- Application Security: It aims to protect applications and provides a degree of security and protection from defects that may arise from design, development or installation defects.

Cyber Security Requirements:

Kennedy (2017) believes that there are a number of basic requirements for the success of Cyber Security, and among these elements:

- Physical elements: These are devices, technical and electronic parts, and tools that represent the necessary infrastructure for the operation of information systems.
- Software components: These are the non-physical components that include the basic software required to operate the systems.
- Human elements: They are people with competence and skills in the field of information technology, and they are interested in operating and updating systems, and maintaining the continuity and continuity of work.
- Support for the top management of the organization:
- Flexibility of the organizational structure and non-resistance to change.

Cyber Security Objectives (Al-Janabi, 2017):

- Ensure the continuity of applications and information systems.
- Updating information systems and protecting them from external risks.
- Work to protect the privacy and confidentiality of information in all its forms.
- Use the necessary measures in order to protect citizens from the risks arising from the use of the Internet.
- Protect operational and technical devices from cybercrime.
- Maintaining the information network.

The Importance of Cyber Security:

The imposition of falling as a victim of cybercrime is increasing day by day, in light of the lack of sufficient awareness, and reliance on the use of the World Wide Web in all aspects of life, especially The Dimension relying on digital transformation (Shiling ford & Stewarb, 2011). This confirms the importance of cybersecurity that it has a number One of the advantages and the primary task of cybersecurity is to maintain the confidentiality of data and protect its privacy, and (Al-Janabi, 2017) believes that the name of the user and the request to verify his identity is the basis for preventing the access of unauthorized persons to view the data, and cybersecurity is also concerned with maintaining the unity of Information by preventing tampering with it, and (Al-Wakil, 2017) adds that there are a number of advantages:

- The ability to save costs in return for high quality and accurate results.
- Remote work, ensuring protection from risks.
- Identify the amount of deviation in performance.
- Save time for comprehensiveness and integration of results.

Cyber Risks:

Cyber risks are represented in all practices that have a criminal purpose in cyberspace and that target individuals, institutions, and governments. According to (Tiwari. et al, 2016), they can be classified into two parts, where the first part targets digital devices and information networks, and the other: targets individuals who use the Internet personally. Or within their various functions in governments.

Among the forms of cyber risks are viruses, cyberbullying, defamation, hacking, and phishing, and according to 2022 statistics, 28% of cyber-attacks on data involved the use of viruses and 52% of attacks involved hacking techniques (Information and Decision Support Center, 2020) and these can be clarified The risks are as follows:

- **Viruses**: They are harmful computer programs that are transmitted through digital devices in several ways, and they spread between files and constitute extremely serious damage, and they vary in their forms, strength and continuation within the digital system, and their danger can reach the point of destroying the digital environment and disrupting its movement (tochi. Et al 2012) .
- **Electronic Bullying**: Electronic bullying is the most prevalent forms of cybercrime, especially among school and university students, and it is classified as a form of digital harassment; Where the victim is harmful for a long time, and he is pursued, controlled by his actions, and the victim threatens to harm, scandal and contempt, and it has spread in the past years significantly. (MENESINI. & Nocentini, 2009)
- **Reputation**: where the victim is aimed at spreading incorrect information and abusing the person and reducing his position using incorrect images or videos that have been treated to serve the crime goals, and send them through social media or e -mail, and it can also aim to distort institutions also with the intention of reducing Its competitive position on the market. (Nathaanael J.2012)
- **Piracy**: It is the process of unauthorized entry in digital information systems with the aim of breaking the security protections of information systems and obtaining secret information and data, whether for individuals, institutions or governments, and causing their loss (Hall & Watson. (2016
- **Hunting**: It is one of the easiest cyber risks in preparation; Where the construction creates a website (for unknown institutions or companies) and sends messages via e -mail from those sites for the purpose of obtaining personal data and information that is used for criminal purposes (Vayansky. & Kumar / 2018)
- **Internet Terrorism**: Terrorist organizations use the Internet to implement a wide variety of purposes that include: recruitment, financing, advertising, training, incitement to commit terrorist acts, collecting and publishing information for terrorist purposes. The Internet is also used to facilitate communication between all terrorist organizations (United Nations, 2013)
- **Violation Of Information Security**: All the uses of information systems and their digital applications loaded on computers are exposed to harmful attacks or failure and disclose the confidentiality of their information or not to save the privacy of the data of the bodies and those dealing with them or delay in their availability at the appropriate time for those who need it quickly, that is, there are many risks to access Unintended, inappropriate and unoccupied use, or the failure of the same systems for side causes, knowing that many information systems and applications, whether public or private, such as those used in military and security purposes, banks, hospitals, and others represent a fertile ground for growing information terrorism today (Al -Hadi, 2006)
- **Intellectual Evidence**: The damage resulting from placing the name of the plaintiff includes scientific work, forging the author's seal, and assaulting any of the rights of the author or neighboring rights (Al-Manthari and Hariri, 2020).

Methods of Protection from Cyber Risks:

One of the most important means of protection that must be followed and applied to address cyber risks is to develop awareness among Internet users of how to use safely through networks. After many cases of cyber-attacks occurred in many countries that targeted schools, universities and other institutions, the matter required the Ministry to play a clear role in planning for cyber security. To protect its environment from these attacks.

Second- Ministry of Interior and National Security:

It is one of the most important ministries in the Palestinian government, bearing complex responsibilities under intertwined conditions, difficult data and multiple security and political crises, as it contributed to finding solutions to many problems, providing an appropriate work environment, finding appropriate alternatives, developing work and facilitating administrative operations and procedures. The Ministry must impose the rule of law on everyone without discrimination or favoritism, control the security situation, provide security for the citizen, and protect the internal front - and to address the events and security crises. The Ministry of Interior received the attention and care of the Palestinian political leadership as one of the most important political ministries for its role in providing security and safety for the Palestinian citizen, and it undertakes important changes and seeks to develop new leaders in order to implement its role, a more comprehensive security service for the Palestinian public.

The Ministry of Interior and National Security consists of two civil and military parts, and the civil part is represented by a number of agents, assistants, departments, directorates, and some public departments such as: the General Administration of Passports and the General Administration of Tribes Affairs, in addition to the competent units that belong to the minister directly, or belong to the ministry’s agent.

As for the security part, which is the subject of the research, it is represented by the competent agencies, departments and security bodies of the ministry, and some of them are followed directly to the minister and some of them are affiliated with the Commander -in -Chief of the National Security Forces (http://www.moi.gov.ps Accessed 2/11/2022).

Methodology and Procedures

The study’s methodology and procedures are considered a main axis through which the applied aspect of the study is accomplished. Accordingly, the researchers will address in this chapter the procedures that were followed in preparing the study by clarifying the study’s approach and its community and then determining the sample on which the study was applied, as well as preparing a tool The main study (the questionnaire) and the mechanism of its construction, development, validity and reliability, and the chapter ends with the statistical treatments that were used in analyzing the data and drawing conclusions.

First- Study Methodology: The researchers used the analytical descriptive approach in order to achieve the objectives of the study, through which it tries to describe the phenomenon under study, analyze its data, and the relationship between its components and the opinions that are raised about it and the processes that it includes. According to (Al-Assaf, 2000), the descriptive analytical approach did not stop at collecting information to describe the phenomenon, but rather went beyond that to clarifying the relationship and its amount, and deducing the reasons behind a certain behavior from previous data.

Second- Study Population And Sample: The study population is considered to be all the vocabulary of the phenomenon that the researchers will carry out its study on (Abu Al-Hasani, 2017) and through the problem of the study and its objectives, the target study community consists of workers in computer and information technology units and departments at the Ministry of Interior and National Security, and for Data collection for the study was done using the simple random sampling method.

Third- Study Tool: We consider the questionnaire as the most widely used and widespread tool among researchers, and the questionnaire is defined as "a tool that includes a number of dimensions, axes, and paragraphs used to obtain opinions or data by a group of respondents according to certain controls, and the respondents respond by themselves to it, which is written.

Table 1: Scores of the scale used in the questionnaire

Response	Strongly Disagree	←								Strongly Agree
Degree	1	2	3	4	5	6	7	8	9	10

Validity of the Study Tool

The validity of the questionnaire reflects the measurement of the paragraphs of the questionnaire, what it was prepared to measure. The validity of the questionnaire has been verified through the following:

The Veracity of the Arbitrators "Virtual Honesty":

The researchers presented the study tool in its initial form to a group of arbitrators from among the specialists. Among the axes of the study, in addition to suggesting what they deem necessary to amend or delete the wording of the phrases, and based on the observations made by the arbitrators, the researchers made the amendments agreed upon by the arbitrators.

Internal Consistency Validity: It means "the extent to which each paragraph of the questionnaire is consistent with the axis to which this paragraph belongs. It was calculated on the sample of the exploratory study of (20) questionnaires, by calculating the correlation coefficients between each paragraph and the total score of the axis to which it belongs.

A. The Results Of The Validity Of The Internal Consistency To Dimensions Of The Reality Of The Application Of Cybersecurity:

- **The First Dimension: Organizational Efforts:**

The following table shows the correlation coefficients between each paragraph of the dimension: organizational efforts and the overall degree of the dimension, which shows the correlation coefficients are statistically significant, as the probability value (Sig) is less than (0.05), and thus it turns out that the paragraphs of the dimension are true.

Table 2: The validity of the internal consistency of the dimension: “Organizational Efforts”

#	Item	Correlation Coefficient	Probability Value
1.	A clear strategy on cyber security is prepared and implemented.	0.862	*0.000
2.	The Department of the Interior and Homeland Security develops computer systems periodically to improve cyber security.	0.884	*0.000
3.	The Ministry of Interior and National Security follows up developments in everything related to protecting systems and networks.	0.907	*0.000
4.	The Ministry of Interior and National Security provides a budget for improving the digital transformation system and activating and improving the cybersecurity system.	0.856	*0.000
5.	The Ministry of Interior and National Security organizes specialized training courses related to the cyber security management system to improve skills.	0.872	*0.000

* The correlation is statistically significant at (α ≤ 0.05).

- **The Second Dimension: Technical Efforts:**

The following table shows the correlation coefficients between each of the paragraphs of the dimension: technical efforts and the total degree of the dimension, which shows the correlation coefficients are statistically significant, as the probability value (Sig) is less than (0.05), and thus it turns out that the paragraphs of the dimension are true.

Table 3: The validity of the internal consistency of the dimension: “Technical Efforts”

#	Item	Correlation Coefficient	Probability Value
1.	The Ministry of Interior and National Security uses a protection network capable of detecting all threats.	0.887	*0.000
2.	The Ministry of Interior and National Security updates protection systems periodically to reduce crimes related to cybersecurity.	0.950	*0.000
3.	Software to protect systems and networks is commensurate with the nature of the work in the ministry.	0.888	*0.000
4.	The Ministry of Interior and National Security develops the database and protection systems related to security and protection on a regular basis.	0.894	*0.000

* The correlation is statistically significant at (α ≤ 0.05).

- **The Third Dimension: Efforts To Monitor Threats:**

The following table shows the correlation coefficients between each item of the dimension: efforts to monitor threats and the overall degree of the dimension, which shows the correlation coefficients are statistically significant, as the probability value (Sig) is less than (0.05), and thus it turns out that the paragraphs of the dimension are true.

Table 4: Validity of the internal consistency of the dimension: “Efforts to monitor threats”

#	Item	Correlation Coefficient	Probability Value
1.	The Ministry of Interior and National Security develops the infrastructure in order to facilitate digital transformation and develop the cybersecurity management system.	0.829	*0.000
2.	The information network used by the Ministry of Interior and National Security is able to reduce crimes related to the Department of Cyber Security.	0.741	*0.000
3.	The Ministry of Interior and National Security uses all that is new in terms of protection systems.	0.878	*0.000
4.	The Department of the Interior and Homeland Security cooperates with outside organizations to reduce penetration of network systems.	0.923	*0.000

* The correlation is statistically significant at (α ≤ 0.05).

- **Fourth Dimension: Laws And Legislations:**

The following table shows the correlation coefficients between each paragraph of the Dimension: Laws and Legislations and the overall degree of the dimension, which shows the correlation coefficients are statistically significant, as the probability value (Sig) is less than (0.05), and thus it turns out that the paragraphs of the dimension are true.

Table 5: The validity of the internal consistency of the dimension: “Laws and Legislations

#	Item	Correlation Coefficient	Probability Value
1.	There are laws and regulations at the Ministry of Interior and National Security that allow the improvement and development of Cyber Security management.	0.690	*0.000

#	Item	Correlation Coefficient	Probability Value
2.	There are legislations and regulations at the Ministry of Interior and National Security that facilitate the process of exchanging information regarding cyber security management with public and private sector institutions.	0.822	*0.000
3.	There are specific instructions and laws on the basis of which citizens and institutions are directed.	0.609	*0.000
4.	The current laws, legislation and regulations of the Ministry of Interior facilitate the management of cyber security.	0.812	*0.000
5.	The laws and legislations of the Ministry of Interior are continuously developed in line with the development of cyber security.	0.663	*0.000

* The correlation is statistically significant at (α ≤ 0.05).

- **The Fifth Dimension: Protecting Privacy:**

The following table shows the correlation coefficients between each of the paragraphs of the dimension: privacy protection and the overall degree of the dimension, which shows the correlation coefficients are statistically significant, as the probability value (Sig) is less than (0.05), and thus it turns out that the paragraphs of the dimension are true.

Table 6: Validity of internal consistency for the dimension: "protecting privacy"

#	Item	Correlation Coefficient	Probability Value
1.	Security gaps in the field of Cyber Security are due to the lack of experience of the public who benefit from the ministry's electronic services.	0.696	*0.000
2.	The inclusion of scientific courses in schools and universities in the field of Cyber Security contributes to the reduction of electronic threats.	0.764	*0.000
3.	Presenting programs through various media to enlighten the public about the most important developments in the field of information security protection.	0.564	*0.000
4.	Review the programs used and the protection at the Ministry on an ongoing basis to ensure the required protection and fill security gaps	0.686	*0.000

* The correlation is statistically significant at (α ≤ 0.05).

1. **Structural Honesty:** Structural validity is considered one of the measures of the validity of the tool and measures the extent to which the goals are achieved, and it shows the extent to which each axis of the study is related to the total score of the questionnaire items, and the following table shows that the correlation coefficients for each axis are statistically significant, as the probability value (Sig) is less than (0.05), Thus, the axes of the study are considered true in their representation of what was set to be measured.

Table 7: Structural validity of the questionnaire axes

The Hub	Correlation Coefficient	Probability Value
The Reality Of Cyber Security		
Organizational Efforts	0.932	*0.000
Technical Efforts	0.969	*0.000
Threat Monitoring Efforts	0.925	*0.000
Rules And Regulations	0.808	*0.000
Privacy Protection	0.552	*0.000

Stability of the Study Tool

"The stability of the questionnaire means that it gives the same result if it is re-applied more than once under the same circumstances, or in other words, the stability of the questionnaire means the stability of the results of the questionnaire and not changing it significantly if it was redistributed several times during certain periods of time, and it has been calculated The stability of the resolution in two ways:

1. **Consistency By Cronbach's Alpha Coefficient:** The following table shows that all Cronbach's alpha coefficients are high, as the digital transformation axis obtained a coefficient of 0.896, while the cyber security axis obtained a stability coefficient of 0.942, and this indicates that the resolution has a high stability coefficient.

Table 8: Cronbach's Alpha coefficient for measuring the stability of the resolution

The Hub	Number Of Vertebrae	Cronbach's Alpha Coefficient
The Reality Of Cyber Security	22	0.942
Organizational Efforts	5	0.869
Technical Efforts	4	0.915
Threat Monitoring Efforts	4	0.800

Rules And Regulations	5	0.713
Privacy Protection	4	0.695

2. **Stability by Split-Half Method:** The test items were divided into two parts, which are the questions with odd numbers and the questions with even numbers, then the correlation coefficient was calculated between the scores of the odd questions and the scores of the even questions, and then the correlation coefficient was corrected by the Spearman Brown equation.

Corrected correlation coefficient = $\frac{2r}{1+r}$ where r is the correlation coefficient between the scores of the odd questions and the scores of the paired questions.

The following table shows that the value of the corrected correlation coefficient (Spearman Brown) is high and statistically significant, and this indicates that the questionnaire has a high stability coefficient.

Table 9: Partition half method to measure the stability of the resolution

The Hub	Correlation Coefficient Before Modification	Corrected Correlation Coefficient
The Reality Of Cyber Security	**0.911**	**0.953**
Organizational Efforts	0.716	0.827
Technical Efforts	0.910	0.953
Threat Monitoring Efforts	0.767	0.868
Rules And Regulations	0.661	0.751
Privacy Protection	0.375	0.545

We note from the previous table that all stability coefficients were high, as the cybersecurity axis obtained a stability coefficient of 0.953, and this indicates that the questionnaire has a high stability coefficient.

Data Analysis, Testing and Discussion of Study Hypotheses

First: The Statistical Description of the Study Sample

The following tables show the statistical description of the study sample according to different variables: gender, age group, educational qualification, years of experience, and job title.

Table 10: shows the distribution of the study sample according to personal and organizational data

		Frequency	Percent	Valid Percent	Cumulative Percent
Age Group	Less than 30 years old	2	3.3	3.3	3.3
	30- Less than 35 years old	5	8.2	8.2	11.5
	35- Less than 40 years old	14	23.0	23.0	34.4
	40 years and over	40	65.6	65.6	100.0
Total		61	100.0	100.0	
Qualification	BA	38	62.3	62.3	62.3
	Master's	20	32.8	32.8	95.1
	Ph.D.	3	4.9	4.9	100.0
Total		61	100.0	100.0	
Years Of Service	Less than 5 years	1	1.6	1.6	1.6
	5- Less than 10 years	9	14.8	14.8	16.4
	10- Less than 15 years old	18	29.5	29.5	45.9
	More than 15 years	33	54.1	54.1	100.0
Total		61	100.0	100.0	
Military Rank	Major	24	39.3	39.3	39.3
	Presenter	29	47.5	47.5	86.9
	Colonel	6	9.8	9.8	96.7
	Major General	2	3.3	3.3	100.0
Total		61	100.0	100.0	
Job Title	Director General	3	4.9	4.9	4.9
	Director Of The Department	19	31.1	31.1	36.1
	Unit Manager	12	19.7	19.7	55.7
	Head Of The Department	27	44.3	44.3	100.0
Total		61	100.0	100.0	

Through the results shown in the previous table, it was found that 65.6% of the study sample were (40 years and over), while 23.0% were between (35 to less than 40 years), and 8.2% were between (30 to less than 35 years), while 3.3% are (30 years or less). The researchers attribute the increase in the number of workers with older ages to the nature of work in supervisory positions in the ministry, which requires older ages.

The results shown in the previous table show that 62.3% of the study sample have a bachelor's degree, while 32.8% have a master's degree, and 4.9% have a doctorate. The researchers attribute this to the nature of work in the Ministry of Interior that requires a bachelor's degree.

Through the results shown in the previous table, it was found that 54.1% of the study sample had years of service (15 years or more), while 29.5% of their years of service ranged from (10 to less than 15 years), and 14.8% of their years of service ranged from (5 to less than 10 years), while 1.6% had years of service (5 years or less). The researchers attribute the high number of workers with experience (15 years or more) to the nature of ranks in the Ministry of Interior, which require long years of experience for promotion.

Through the results shown in the previous table, it was found that 47.5% of the study sample held the rank of lieutenant colonel, while 39.3% held the rank of major, 9.8% held the rank of colonel, while 3.3% held the rank of major general. The researchers attribute this to the nature of the organizational pyramid in the security institutions.

Through the results shown in the previous table, it was found that 44.3% of the study sample were named department heads, while 31.1% were named department directors, 19.7% were named unit directors, while 4.9% were named deputy directors. The researchers attribute this to the nature of the organizational hierarchy in the security institutions.

Second: Analyzing the Axes of the Questionnaire

The researchers used the appropriate descriptive tests: arithmetic means, standard deviations, relative weights, and rankings for the dimensions of cybersecurity and the total score, then the researchers analyzed the data of each dimension of cybersecurity separately.

Table 11: Arithmetic means, standard deviations, relative weights, and rankings for each axis of cybersecurity dimensions and the total score

#	The Dimension	SMA	Standard Deviation	Relative Weight(%)	Rank
1.	Organizational Efforts	7.3410	1.89115	73.4	4
2.	Technical Efforts	7.4795	1.77030	74.8	2
3.	Threat Monitoring Efforts	7.3443	1.85470	73.4	4
4.	Rules And Regulations	7.4098	2.01806	74.1	3
5.	Privacy Protection	7.8443	1.58191	78.4	1
Total Degree		7.4838	1.74337	74.8	

It can be seen from the previous table that "the relative weight of the total score of the respondents' responses to the cybersecurity items came to a large degree and amounted to (74.8%), and the privacy protection dimension ranked first with a relative weight of (78.4%), while the technical efforts dimension came in the second rank with a relative weight of (74.8%). %), then The Dimension laws and legislations in the third rank with a relative weight of (74.1%), while The Dimension efforts to monitor threats and The Dimension organizational efforts came in the fourth and fifth rank with a relative weight of (73.4%).

The researchers attribute this to the interest of the Ministry of Interior in cybersecurity through the availability of all the necessary privacy protection for the data that the ministry deals with and the provision of appropriate technical efforts with the enactment of laws and legislation that protect the privacy of data and the monitoring of any threats that may occur to the data through the organizational efforts available in the ministry.

The following tables illustrate the analysis of each dimension of cybersecurity:

A. Paragraph Analysis The Dimension: “Organizational Efforts”:

Table 12: Paragraph Analysis: “The Dimension Organizational Efforts”

#	Item	SMA	Standard Deviation	Relative Weight(%)	Rank
1.	A clear strategy on cyber security is prepared and implemented.	7.46	1.954	74.6	2
2.	The Department of the Interior and Homeland Security develops computer systems periodically to improve cyber security.	7.41	2.077	74.1	3
3.	The Ministry of Interior and National Security follows up developments in everything related to protecting systems and networks.	7.48	1.920	74.8	1
4.	The Ministry of Interior and National Security provides a budget for improving the digital transformation system and activating and improving the cybersecurity system.	7.08	2.155	70.8	5
5.	The Ministry of Interior and National Security organizes specialized training courses related to the cyber security management system to improve skills.	7.28	1.881	72.8	4
Total Degree		7.3410	1.89115	73.4	

The following is evident from the previous table:

- The paragraph stating: The Ministry of Interior and National Security follows up on developments in everything related to the protection of systems and networks” ranked first among the rest of the paragraphs with a relative weight of (74.8%), and this indicates a high degree of approval for this paragraph.
- The paragraph that states: The Ministry of Interior and National Security provides a budget for improving the digital transformation system and activating and improving the cybersecurity system got the last ranking among the rest of the paragraphs with a relative weight of (70.8%), and this indicates that there is a high degree of approval for this paragraph.
- In general, "the relative weight of the dimension: organizational efforts reached (73.4%), which indicates that this axis enjoys a high degree of approval."

The researchers attribute this to the workers' feeling of satisfaction with the ministry's organizational efforts towards enhancing cybersecurity.

B. Paragraph Analysis The Dimension: "Technical Efforts":

Table 13: Paragraph Analysis: “The Dimension Technical Efforts”

#	Item	SMA	Standard Deviation	Relative Weight(%)	Rank
1.	The Ministry of Interior and National Security uses a protection network capable of detecting all threats.	7.31	1.962	73.1	4
2.	The Ministry of Interior and National Security updates protection systems periodically to reduce crimes related to cybersecurity.	7.49	1.850	74.9	3
3.	Software to protect systems and networks is commensurate with the nature of the work in the ministry.	7.56	1.766	75.6	1
4.	The Ministry of Interior and National Security develops the database and protection systems related to security and protection on a regular basis.	7.56	1.812	75.6	1
Total Degree		7.4795	1.77030	74.8	

The following is evident from the previous table:

- The paragraph stating: Systems and network protection software is commensurate with the nature of the work in the ministry, and the paragraph “The Ministry of Interior and National Security develops the database and protection systems related to security and protection on a regular basis” got the first rank among the rest of the paragraphs with a relative weight (75.6%), This indicates that there is a large degree of approval for this paragraph."
- The paragraph stating: The Ministry of Interior and National Security uses a protection network capable of detecting all threats” got the last ranking among the rest of the paragraphs with a relative weight of (73.1%), and this indicates a high degree of approval for this paragraph.
- In general, "the relative weight of the dimension: technical efforts reached (74.8%), which indicates that this axis enjoys a high degree of approval."

The researchers attribute this to the workers' feeling that the ministry is making great technical efforts to implement cyber security by providing appropriate and advanced devices and software that protect data and prevent hacking.

C. Analysis Of The Paragraphs The Dimension: “Efforts To Monitor Threats:

Table 14: Analysis of paragraphs: “The Dimension Efforts to Monitor Threats”

#	Item	SMA	Standard Deviation	Relative Weight(%)	Rank
1.	The Ministry of Interior and National Security develops the infrastructure in order to facilitate digital transformation and develop the cybersecurity management system.	7.49	1.955	74.9	1
2.	The information network used by the Ministry of Interior and National Security is able to reduce crimes related to the Department of Cyber Security.	7.43	1.901	74.3	2
3.	The Ministry of Interior and National Security uses all that is new in terms of protection systems.	7.31	2.029	73.1	3
4.	The Department of the Interior and Homeland Security cooperates with outside organizations to reduce penetration of network systems.	7.15	2.136	71.5	4
Total Degree		7.3443	1.85470	73.4	

The following is evident from the previous table:

- The paragraph that states: The Ministry of Interior and National Security develops the infrastructure in order to facilitate digital transformation and develop the cybersecurity management system.” It ranks first among the rest of the paragraphs with a relative weight of (74.9%), and this indicates a high degree of approval for this paragraph. ".
- The paragraph that states: The Ministry of Interior and National Security cooperates with external institutions to limit penetration of network systems” got the last ranking among the rest of the paragraphs with a relative weight (71.5%), and this indicates that there is a high degree of approval for this paragraph.
- In general, "the relative weight of the dimension: Efforts to monitor threats was (73.4%), which indicates that this axis enjoys a high degree of approval."

The researchers attribute this to the Ministry's relentless endeavor to monitor the threats that the information system in the Ministry may be exposed to, as it contains sensitive and important parameters related to the Ministry's work.

D. Analysis Of The Paragraphs The Dimension: “Laws And Legislations:

Table 15: Analysis of Paragraphs: “The Dimension Laws and Legislations:

#	Item	SMA	Standard Deviation	Relative Weight(%)	Rank
1.	There are laws and regulations at the Ministry of Interior and National Security that allow the improvement and development of Cyber Security management.	7.38	2.001	73.8	4
2.	There are legislations and regulations at the Ministry of Interior and National Security that facilitate the process of exchanging information regarding cyber security management with public and private sector institutions.	7.48	2.241	74.8	2
3.	There are specific instructions and laws on the basis of which citizens and institutions are directed.	7.57	1.945	75.7	1
4.	The current laws, legislation and regulations of the Ministry of Interior facilitate the management of cyber security.	7.41	2.124	74.1	3
5.	The laws and legislations of the Ministry of Interior are continuously developed in line with the development of cyber security.	7.21	2.222	72.1	5
Total Degree		7.4098	2.01806	74.1	

The following is evident from the previous table:

- The paragraph that states: There are specific laws and instructions on which citizens and institutions are directed.” It got the first rank among the rest of the paragraphs with a relative weight of (75.7%), and this indicates a high degree of approval for this paragraph.
- The paragraph that states: The laws and legislations of the Ministry of the Interior are being developed continuously in line with the development of cybersecurity.” It got the last ranking among the rest of the paragraphs with a relative weight of (72.1%), and this indicates that there is a high degree of approval for this paragraph.
- In general, "the relative weight of the dimension: laws and legislation was (74.1%), which indicates that this dimension enjoys a high degree of approval."

The researchers attribute this to the ministry's efforts to issue clear laws and regulations to help workers maintain the security of data and information in a way that prevents them from being hacked.

E. Analysis Of The Following Paragraphs: Privacy Protection:

Table 16: Analysis of Paragraphs: “After Privacy Protection”

#	Item	SMA	Standard Deviation	Relative Weight(%)	Rank
1.	Security gaps in the field of Cyber Security are due to the lack of experience of the public who benefit from the ministry's electronic services.	7.59	1.657	75.9	4
2.	The inclusion of scientific courses in schools and universities in the field of Cyber Security contributes to the reduction of electronic threats.	8.10	1.609	81.0	1
3.	Presenting programs through various media to enlighten the public about the most important developments in the field of information security protection.	7.90	1.777	79.0	2

#	Item	SMA	Standard Deviation	Relative Weight(%)	Rank
4.	Review the programs used and the protection at the Ministry on an ongoing basis to ensure the required protection and fill security gaps	7.79	1.993	77.9	3
Total Degree		7.8443	1.58191	78.4	

The following is evident from the previous table:

- The paragraph stating: Including scientific courses in schools and universities in the field of Cyber Security contributes to reducing electronic threats. "I got the first rank among the rest of the paragraphs with a relative weight of (81.0%), and this indicates that there is a high degree of approval for this paragraph." ".
- The paragraph that states: security gaps in the field of Cyber Security is due to the lack of experience of the public who benefit from the Ministry's e-services." It got the last ranking among the rest of the paragraphs with a relative weight of (75.9%), and this indicates that there is a high degree of approval for this paragraph. ".
- In general, "the relative weight of the dimension: protection of privacy was (78.4%), which indicates that this dimension enjoys a high degree of approval."

The researchers attribute this to the ministry's endeavor to provide and protect privacy by providing a username and password for each user, while defining specific access rights to the system that cannot be bypassed.

Conclusions

The following Results and recommendations were reached:

- The results of the study showed that there was a great deal of agreement with the degree of Cyber Security application, which amounted to (74.8%).
- The results of the study showed that The Dimension the regulatory efforts it had a great approval degree and a relative weight of (73.4%).
- The results of the study indicated that The Dimension the technical efforts it obtained a large approval degree and a relative weight of (74.8%).
- The results of the study indicated that The Dimension efforts to monitor threats, it obtained a high degree of approval and a relative weight of (73.4%).
- The results of the study indicated that The Dimension the laws and legislations, it had a great approval degree and a relative weight of (74.1%).
- The results of the study indicated that the privacy protection dimension obtained a large approval degree and a relative weight of (78.4%).

Recommendations

- Interest in providing the Ministry of Interior and National Security with a budget to improve the digital transformation system and activate and improve the Cyber Security system.
- The need for the Ministry of Interior and National Security to use a protection network capable of detecting all threats.
- The Ministry of Interior and National Security cooperates with external institutions to limit penetration of network systems.
- Continuously strengthening and developing the laws and legislations of the Ministry of Interior in line with the development of cyber security.
- Enhancing the experiences of the beneficiaries of the Ministry's electronic services to reduce security gaps in the field of Cyber Security.

Acknowledgment

The authors extend their sincere thanks and appreciation to all who enriched the current study with valuable information, without which the study would not have appeared in its present elegant form.

References

[1]Abu Naser, S. S. and M. J. Al Shobaki (2017). "The Impact of Senior Management Support in the Success of the e-DMS." International Journal of Engineering and Information Systems (IJEAIS) 1(4): 47-63.

[2]Abu-Nahel, Z. O., et al. (2020). "The Reality of Applying Strategic Flexibility in Non-Governmental Hospitals." International Journal of Academic Management Science Research (IJAMSR) 4(7): 144-170.

[3]Abusharekh, N. H., et al. (2020). "The Impact of Modern Strategic Planning on Smart Infrastructure in Universities." International Journal of Academic Management Science Research (IJAMSR) 4(8): 146-157.

[4]Al Shobaki, M. J. and S. S. Abu Naser (2016). "Decision support systems and its role in developing the universities strategic management: Islamic university in Gaza as a case study." International Journal of Advanced Research and Development 1(10): 33-47.

[5]Al Shobaki, M. J., et al. (2016). "The impact of top management support for strategic planning on crisis management: Case study on UNRWA-Gaza Strip." International Journal of Academic Research and Development 1(10): 20-25.

[6]Al Shobaki, M. J., et al. (2017). "Impact of Electronic Human Resources Management on the Development of Electronic Educational Services in the Universities." International Journal of Engineering and Information Systems 1(1): 1-19.

[7]Al Shobaki, M. J., et al. (2017). "Strategic and Operational Planning As Approach for Crises Management Field Study on UNRWA." International Journal of Information Technology and Electrical Engineering 5(6): 43-47.

[8]Al Shobaki, M. J., et al. (2017). "The Reality of the Application of Electronic Document Management System in Governmental Institutions-an Empirical Study on the Palestinian Pension Agency." International Journal of Engineering and Information Systems 1(2): 1-14.

[9]Al Shobaki, M. J., et al. (2018). "Support Extent Provided by Universities Senior Management in Assisting the Transition to e-Management." International Journal of Academic Management Science Research (IJAMSR) 2(5): 1-26.

[10]Al Shobaki, M. J., et al. (2018). "The Entrepreneurial Creativity Reality among Palestinian Universities Students." International Journal of Academic Management Science Research (IJAMSR) 2(3): 1-13.

[11]Al Shobaki, M. J., et al. (2018). "The Extent to Which Technical Colleges Are Committed To Applying Lean Management." International Journal of Engineering and Information Systems (IJEAIS) 2(1): 23-42.

[12]Al Shobaki, M. J., et al. (2019). "The Role of Human Resources in Interpreting the Relation between the Emphases on the Operations Standard and Improving the Overall Performance of the Palestinian Universities." International Journal of Academic Management Science Research (IJAMSR) 3(5): 60-75.

[13]Al Shobaki, M. J., et al. (2020). "Digital Repositories and Their Relationship to the Modern Strategic Planning of the Universities' Smart Infrastructure." International Journal of Academic Information Systems Research (IJAISR) 4(9): 1-18.

[14]Al Shobaki, M. J., et al. (2020). "Digital Reputation in the University Of Palestine: An Analytical Perspective of Employees' Point Of View." International Journal of Academic Accounting, Finance & Management Research (IJAAFMR) 4(9): 22-37.

[15]Al Shobaki, M. J., et al. (2020). "Measuring the E-Content of the Digital Repositories in the University of Palestine." International Journal of Academic Information Systems Research (IJAISR) 4(10): 34-50.

[16]Al Shobaki, M. J., et al. (2020). "The Reality of Using Digital Repositories at the University of Palestine." International Journal of Academic Accounting, Finance & Management Research (IJAAFMR) 4(8): 115-134.

[17]Alayoubi, M. M., et al. (2020). "Requirements for Applying the Strategic Entrepreneurship as an Entry Point to Enhance Technical Innovation: Case Study-Palestine Technical College-Deir al-Balah." International Journal of Business and Management Invention (IJBMI) 9(3): 1-17.

[18]Alayoubi, M. M., et al. (2020). "Strategic Leadership Practices and their Relationship to Improving the Quality of Educational Service in Palestinian Universities." International Journal of Business Marketing and Management (IJBMM) 5(3): 11-26.

[19]Almasri, A., et al. (2018). "The Organizational Structure and its Role in Applying the Information Technology Used In the Palestinian Universities-Comparative Study between Al-Azhar and the Islamic Universities." International Journal of Academic and Applied Research (IJAAR) 2(6): 1-22.

[20]Arqawi, S. M., et al. (2019). "Strategic Orientation and Its Relation to the Development of the Pharmaceutical Industry for Companies Operating in the Field of Medicine in Palestine." International Journal of Academic Management Science Research (IJAMSR) 3(1): 61-70.

[21]Catota. Frankie. Morgan. Granger. & Sicker Douglasmar. (2019): Cyber Security education in developing nation: the Ecuadorian environment. Journal of CYBER SECURITY. 119

[22]El Talla, S. A., et al. (2018). "Organizational Structure and its Relation to the Prevailing Pattern of Communication in Palestinian Universities." International Journal of Engineering and Information Systems (IJEAIS) 2(5): 22-43.

[23]El Talla, S. A., et al. (2018). "The Availability of the Focus Standards on Human Resources and Processes as a Potential for Excellence in Palestinian Universities According to the European Model." International Journal of Academic Management Science Research (IJAMSR) 2(11): 58-69.

[24]El Talla, S. A., et al. (2018). "The Nature of the Organizational Structure in the Palestinian Governmental Universities-Al-Aqsa University as A Model." International Journal of Academic Multidisciplinary Research (IJAMR) 2(5): 15-31.

[25]El Talla, S. A., et al. (2019). "Intermediate Role of the Focus Standard on Human Resources in the Relationship between Adopting the Criterion of Leadership and Achieving Job Satisfaction in the Palestinian Universities." International Journal of Academic Management Science Research (IJAMSR) 3(3): 48-60.

[26]FarajAllah, A. M., et al. (2018). "The Reality of Adopting the Strategic Orientation in the Palestinian Industrial Companies." International Journal of Academic Management Science Research (IJAMSR) 2(9): 50-60.

[27]Hamdan, M. K., et al. (2020). "Strategic Sensitivity and Its Impact on Boosting the Creative Behavior of Palestinian NGOs." International Journal of Academic Accounting, Finance & Management Research (IJAAFMR) 4(5): 80-102.

[28]Hamdan, M. K., et al. (2020). "The Effect of Choosing Strategic Goals and Core Capabilities on the Creative Behavior of Organizations." International Journal of Academic Information Systems Research (IJAISR) 4(4): 56-75.

[29]Hamdan, M. K., et al. (2020). "The Reality of Applying Strategic Agility in Palestinian NGOs." International Journal of Academic Multidisciplinary Research (IJAMR) 4(4): 76-103.

[30]Kennedy, C., (2017), the internet of things: The cyber security risks and how to protect against them.

[31]Keshta, M. S., et al. (2020). "Perceived Organizational Reputation and Its Impact on Achieving Strategic Innovation." International Journal of Academic Information Systems Research (IJAISR) 4(6): 34-60.

[32]Keshta, M. S., et al. (2020). "Strategic Creativity and Influence in Enhancing the Perceived Organizational Reputation in Islamic Banks." International Journal of Academic Accounting, Finance & Management Research (IJAAFMR) 4(7): 13-33.

[33]Keshta, M. S., et al. (2020). "Strategic Creativity in Islamic Banks in Palestine between Reality and Implementation." International Journal of Academic Accounting, Finance & Management Research (IJAAFMR) 4(3): 79-98.

[34]Madi, S. A., et al. (2018). "The Organizational Structure and its Impact on the Pattern of Leadership in Palestinian Universities." International Journal of Academic Management Science Research (IJAMSR) 2(6): 1-26.

[35]Maranga Mayieka. & Nelson Masese (2019): Emerging Issues in - Cyber Security for Initiutions of Higher Education. International Journal of Computer Science & Network. 8(4). August 2019.2277-5420.

[36]Menesini. Ersilia & Nocentini. Annalaura (2009): Cyber bullying Definition and Measurement- Some Critical Considerations Zeitschrift fur psychologue. 217(4).

[37]Moskal, E. (2020). A model for establishing a cyber-security center of excellence. Information systems education journal. 13 (6), 97- 108

[38]Nathanael J. Fast. Yeri Cho (2012): Power defensive denigration and the assuaging effect of gratitude expression. Journal of Experimental Social Psychology. 48(3). 778 – 782

[39]Ninkeu, N., Anye, D., Kwededu, L. & Buttler, W. (2018). Cyber education outside the cyber space: the Case of catholic university institute of Buea. International journal of technology in teaching and learning. 14 (2), 90-101.

[40]Richardson. M... Lemoine. P... Stephens W... & waller. R. (2020): Planning for Cyber Security in Schools -The Human Factor. Educational planning.27 (2). 23-39.

[41]Tiwari. Soumya. Bhalla. Anshika. & Rawat. Ritu (2016): Cyber - Crime and Security. International Journal of advanced research in Computer Science and Software engineering. 6(4). 46- 52

[42]vayansky. Ike & Kumar SathishA.p (2018): phishing – Challenges and Solutions. Computer Fraud & Security. (1). 15- 20.

Arabic References in Roman Scripts:

[1]Abu Al-Hasani, Abdullah Mansour (2017). The role of organizational and functional factors in the successful management of NGO projects in Gaza Strip. (Unpublished master's thesis) The Islamic University, Gaza.

[2]Al-Arishi, Jibril, Al-Dosari, Salma (2018). The role of higher education institutions in promoting a culture of Cyber Security in society. King Fahd National Library Journal. Riyadh. (24)2.

[3]Al-Assaf, Saleh bin Hamad. (2000 AD). Handbook for Researchers in the Behavioral Sciences. Riyadh: Obeikan Library.

[4]Al-Bahi, Raghda. (2017). Cyber deterrence concept, problems and requirements. Journal of Political Science. . https://democraticac.de

[5]Al-Janabi, Lily (2017). The effectiveness of national and international laws in combating cybercrime, research published on https://www.ssrcaw.org on 5/9/2017.

[6]Al-Jifnawi, Khaled. (2021). Digital transformation of national institutions and Cyber Security challenges from the point of view of academic police officers in Kuwait. Arab Journal of Arts and Humanities, Arab Foundation for Education, Science and Arts. Volume (5). Issue 19, pg. 75.

[7]Al-Jundi, Alia, Hassan, Nahair Taha (2019). The role of the applied practice of Cyber Security in developing the skills and accuracy of the practical application of information security among university students, Journal of the World of Education. Cairo. The Arab Foundation for Scientific Consultation and Human Resources Development. (67) 3. pp. 14-84.

[8]Al-Manthari, Fatima Yousef (2020) The role of school leadership in enhancing cybersecurity in government schools for girls in Jeddah from the point of view of female teachers, The Arab Journal of Educational and Psychological Sciences, (17) July 4. 48-95, 2020

[9]Al-Manthari, Fatima Youssef, and Hariri, Randa (2020) The degree of awareness of middle school teachers about cybersecurity in public schools in Jeddah from the point of view of female teachers, The Arab Journal for Specific Education, (13), 4 July 2020.

[10]Al-Qahtani, Noura Nasser (2019). The availability of cyber security awareness among male and female Saudi university students from a social perspective. Social Affairs Journal. Sharjah. (36) 144, pp. 85-120.

[11]Al-Sanea, Nora, Suleiman, Enas, Asran, Awatef, Al-Sawat, Hamad, Abu-Aisha, Zahda (2020). Teachers' awareness of Cyber Security and methods of protecting students from the dangers of the Internet and promoting their national values and identity. Journal of the Faculty of Education in Assiut. (26) 6, 41-90.

[12]Al-Wakil, Sami (2017). Cyber Security is a national protection for the security of the individual and society in the Kingdom of Saudi Arabia. Research published on 10/1/2017. https://www.spa.gov.sa.

[13]Bahour, Khaled (2016). The availability of factors affecting the adoption and application of cloud computing in government institutions from the point of view of senior management. (Unpublished master's thesis) The Islamic University, Gaza.

[14]Faraj, Alia (2021). The reasons for enhancing the culture of Cyber Security in light of the digital transformation - Prince Sattam bin Abdulaziz University as a model. Sohag University. Faculty of Education. Part (1).

[15]Information and Decision Support Center (2020). The Most Important Cyber Security Breakthroughs for 2020 Cabinet, Arab Republic of Egypt, December 2020.

[16]Qari, Reem Abdel-Rahim and Al-Sani, Reem Alawi and Allam, Nouf Khaled (2019). Keys to Cybersecurity in Education, Jeddah.

[17]http://www.moi.gov.ps