Training Needs of Information Specialists at Saudi Universities Libraries to Achieve Cybersecurity Requirements

Alia M. Alhaif
Princess Nourah bint Abdulrahman University
Airport Road, King Khalid International Airport, Riyadh 11564,
Kingdom of Saudi Arabia
https://orcid.org/0000-0002-8850-868X

Received: July 9, 2022. Revised: February 21, 2023. Accepted: March 5, 2023. Published: April 5, 2023.

Abstract— This study aimed to determine the cybersecurity degree of awareness among information specialists in Saudi university libraries, their required competencies, the vital training needs, and statistically significant differences in cybersecurity awareness among information specialists according to gender, years of experience, and the number of training courses. The researcher used the descriptive analytical method on a sample of male and female university librarians in Saudi libraries. The sample consisted of 200 information specialists from Saudi universities. The questionnaire included six axes: awareness of cybersecurity among information specialists, cybersecurity systems and methods for information professionals in Saudi university libraries, the necessary cybersecurity competencies for information specialists in Saudi universities, the requirements for achieving cybersecurity, and the training needs for information specialists to achieve cybersecurity. A high degree of relative cybersecurity awareness among information specialists at Saudi universities' libraries was found. Statistically, there were significant differences in gender, years of experience, and training courses.

Keywords— Cyber security, Information Specialist, training needs, Information and communications technology, Saudi Universities.

I. Introduction

UNIITYVERS libraries disseminate knowledge to students at all levels. Information and communication technology has resulted in new developments and updates in cyberspace. Information and communication technologies have continuously advanced. Intrinsic features of gradual computing and the transfer of activities to cyberspace can be found within the work of individuals, companies, and the global community, [1], [2], [3].

Achieving future technological progress goals necessitates assuring the security of data and services deployed in cyberspace. According to EU agencies' investigations, state reports, and business publications on cybersecurity, the magnitude of cyber events has been increasing, [4], [5]. Cyberthreats are growing increasingly sophisticated, involving various attack methods and approaches. As a result of both development and threats, cyberspace is an environment of good and bad cooperation. Maintaining technical advancement while also ensuring cybersecurity is a huge challenge. Many countries' and international organizations' agendas and legislative acts reflect this issue.

Cybersecurity affects every organization and every individual. Digital vulnerabilities pose serious challenges to organizations, governments, businesses, and the broader public—including libraries. From email scams to hacking a library's user database, library systems can become targets—especially with the drain caused by COVID-19.

II. Literature Review

The Kingdom of Saudi Arabia's National Cybersecurity Authority defined cybersecurity as the protection of networks, information technology systems, operational technology systems, their hardware and software components, the services they provide, and the data they contain from any penetration, disruption, entry, use, or illegal exploitation, [6].

All governments and institutions have recently been interested in planning cybersecurity policies because it provides a trustworthy, safe environment, protect digital devices, and guard against cybercrimes, [7].

Cyberhazards are criminal activities in cyberspace that attack persons, institutions, and governments. It is divided into two parts: the first targets digital devices and information networks, while the second targets persons who use the Internet for personal reasons or as part of their varied government tasks, [8]. Viruses, cyberbullying, defamation, hacking, and phishing are examples of cyber risks. According

to 2020 figures, viruses were used in 28% of cyberattacks, and hacking tactics were used in 52% of attacks, [9].

One of the most important means of protection against cyber risks is awareness among Internet users of how to use networks securely. After the occurrence of many cases of cyberattacks in many countries that targeted universities and schools, it was necessary to plan cybersecurity to protect the university environment from these attacks and put forward some of these initiatives, such as a declared action plan targeting how to deal with cyber risks and various violations and to provide training courses for all security personnel on how to raise awareness of cybersecurity and awareness of how to deal when they fall victim to cyber risks.

[10], indicated that organizations lack situational awareness to make informed decisions in the field of cybersecurity, in addition to lacking the necessary resources for implementation.

Moreover, [11], aimed to identify the mechanisms of digital management of universities and coordinate a balance between providing a secure digital environment for all university faculties and achieving this security level. The university provided its own digital application and trained faculty, students, and information specialists .

Furthermore, [12], identified ways to secure universities from cyberattacks. The essential mechanisms were educating faculty members, students, and information specialists in university libraries through exchange programs between universities and conducting conferences, seminars, and workshops that discuss cybersecurity and provide university administrations with digital protection tools .

According to a survey, educational institutions are exposed to cyberattacks at a greater rate than others, [13].

The study by [14], determined the degree of awareness among teachers of cybersecurity in the city of Taif, Kingdom of Saudi Arabia, and the degree of teachers' use of methods and strategies to protect students from the dangers of the Internet to identify the correlation between them. The study concluded that it is necessary to spread a culture of cybersecurity awareness among teachers of all general educational levels to raise awareness of the dangers of the Internet and the importance of preparing training programs on protection methods for teachers, [14].

Many studies, showed that the success of libraries and information facilities in universities depends mainly on the qualification of their employees. With the adoption of educational technology, there must be competencies in those who work in this type of libraries, so that they can carry out its various tasks [15], [16], Furthermore, given the variety of tasks performed by workers in libraries and information facilities in universities, the demand for a wide range of these competencies grows, particularly in light of significant advances in informatics and increasing confidence in the use of information technology in libraries, owing to the benefits of computerization such as saving time, effort, money, and space, making a massive amount of information available via networks, and facilitating communication with publishers and beneficiaries, [17].

[18], identified the behavior, status, and prospects of future libraries in providing librarians with cybersecurity skills to protect against unauthorized access to the data bank. The study results concluded that librarians must rise to the challenge and adopt cybersecurity skills to protect against unauthorized access.

Accordingly, it is necessary to strengthen the concepts and mechanisms of cybersecurity for information specialists in university libraries to protect sensitive data and information and educate the staff about cyber violations and risks and prevention methods, [19].

In 2017, the number of cybersecurity incidents doubled globally, with an increase of about 40% in the number of data security breaches and annual losses of $608 billion, with a total loss rate of $3.9 billion, [20].

Examing the information security awareness of students in the College of Education by [21], the results showed that most students were not sufficiently aware of information security. Moreover, they determined that gender and average duration of computer and Internet use had a significant impact on cybersecurity awareness, whereas information security training status had no effect.

[22], focused on closing the cybersecurity skills gap through interest cultivation and self-determined motivation. The study found that situational interest)SI(in cybersecurity and situational motivational variables, such as perceived learning autonomy, perceived relatedness, and influenced self-determined motivation toward cybersecurity training. As a result, self-determined incentives aided real learning behavior. On the other hand, individual interest in cybersecurity had a positive moderating influence on the links between self-determination and its primary antecedents, namely, perceived relatedness and SI, [22].

Saudi university libraries handle sensitive patron information, such as personally identifying information and circulation records. Libraries that provide services to students must understand the value of patron privacy and how to preserve it.

To investigate how the knowledge transferred within an online cybersecurity education affects the information security practices of library employees, [23]. The results of this study suggest that knowledge transfer benefits the information security and risk management practices of library employees.

[24], examined the cybersecurity behaviors of university students according to five personality traits and variables, such as gender, grade level, department, information security training status, and weekly Internet use. A total of 420 students from different universities, departments, and grade levels participated in the study. This study was conducted according to a descriptive research model. Data were collected using the Personal Information Model developed by the researchers, the Personal Cybersecurity Provision Scale, and the Big Five Traits Scale. Pearson's correlation coefficient, independent

samples t-test, and one-way analysis of variance (ANOVA) were used to analyze the data. The results indicated that the students' cybersecurity behavior levels were acceptable, [24].

While the students perceived themselves as amiable, conscientious, and open to new experiences, they could not determine whether they were extroverted or neurotic. Furthermore, all five personality traits, namely, openness to experience, conscientiousness, agreeableness, neuroticism, and extroversion, were found to be significantly associated with students' cybersafety behaviors. The personality trait with the strongest relationship to cybersecurity behaviors was openness to experience, while extroversion was the weakest. Furthermore, students from the CEIT and Computer Programming departments, those in third and fourth graders, those with information security training, and those who use the Internet 6–10 hours per week were shown to be better qualified regarding cybersecurity behavior. At the end of the study, it was proposed that cybersecurity exercises be prioritized and pupils' particular characteristics be considered.

[25], identified cybersecurity mechanisms in limiting deviant behaviors of events and the efforts of the Kingdom of Saudi Arabia. The ways to help Saudi society reduce juvenile deviant behaviors were generally identified using the scientific approach to cybersecurity, [25].

[26], explored the relationship between students' addiction to social networking sites with psychological security and involvement in cybercrimes. The study sample consisted of 252 students at Taibah University in Madinah. The measures of psychological security and exposure to cybercrime through social media were prepared by the two researchers and social networking sites. Most students had accounts on social media (95.6%), and Snapchat was the most used application (23.0%) for more than four hours a day (48%). There was a negative and predictive correlation with statistical significance between students' addiction to using social networking sites and their psychological security. It seemed that students' use of social networking sites had a positive correlation. It was statistically significantly predictive of the extent of their exposure to cybercrime through these means, and it was found that the students' exposure to cybercrime had a correlative relationship, [26].

[27], revealed the level of cybersecurity awareness among secondary school computer teachers in Jeddah. The study sample included 106 female teachers. There were shortcomings in awareness of the concepts of cybersecurity. Also, there were no statistically significant differences between the average responses of the study sample members in the degree of awareness. The attributed parameters of cybersecurity were years of experience, educational qualification, and training courses [27].

[28], revealed the most critical forms of cyberextortion crimes, their motives, and the related psychological effects according to teachers, staff members, and psychological counselors. The sample included 48 members of the Committee for the Promotion of Virtue and the Prevention of Evil, 48 psychological counselors, and 368 teachers, who were randomly selected. The results of the study indicated statistically significant differences in material, emotional, and entertainment motives between psychological counselors and teachers in favor of teachers and between teachers and men of authority in favor of teachers. At the same time, the differences in sexual motives between teachers and men of authority were in favor of authority men. Finally, the study results showed statistically significant differences in the degree of estimation of the psychological effects of electronic blackmail crimes. It is due to the difference in the respondent category (teachers and psychological counselors) in favor of psychological counselors, [28].

Previous studies indicated the importance of providing security requirements for cybersecurity policies through training, awareness-raising, and educational programs.

The accelerating technological revolution facing library and information sciences is represented in a set of fundamental challenges, including cyberattacks and data breaches, and affects every organization and every individual. Digital vulnerabilities pose serious challenges to organizations, governments, businesses, and the broader public—including libraries. As the scope of threats and the scope of targets for such attacks are rapidly increasing, library systems can become targets. So, securing their digital assets and services is a high priority.

Given the increasing attacks associated with the multiple information systems operating on the university network, increasing the knowledge and awareness of cybersecurity by the information specialist and in university libraries in Saudi Arabia is crucial.

As many studies have indicated, organizations lack situational awareness to make informed decisions in the field of cybersecurity.

Therefore, libraries must use extra care when handling patrons' personally identifiable information.

While information specialists and other library employees recognize the importance of data security, they frequently lack the resources to assess information security risk, implement risk mitigation techniques, and provide security education, training, or awareness (SETA) programs. This is especially concerning because libraries are increasingly gaining access to databases containing both proprietary and personal information. Organizations worldwide implement SETA programs to promote and maintain end-user compliance with information security and privacy regulations. Information systems are commonly utilized in libraries to provide services to users; nevertheless, little is known about library information security policies. Given the sensitivity of the data handled by libraries, it is critical for employees working in or seeking to work in the library setting to develop the knowledge required to recognize risks and implement risk mitigation methods to secure the information entrusted to them.

There seems to be an urgent need for cybersecurity training in universities within the curriculum, and employees should be

supported in such a regard.

III. Research Problem

The accelerating technological revolution facing library and information sciences is represented in a set of fundamental challenges. Digital vulnerabilities pose serious challenges. As the scope of threats and targets for such attacks are rapidly increasing, library systems can become targets, necessitating the security of their digital assets and services.

Few studies found that many organizations lack situational awareness to make informed decisions in cybersecurity.

Information specialists have a low-level cybersecurity awareness, and they lack the application of cybersecurity controls and precautions in university libraries due to their insufficient training. It is necessary to reexamine the aspects related to the qualification of human cadres working in these institutions, especially in light of the trend toward digital transformation in Saudi universities.

Hence, this study aims to know the degree of awareness of information specialists in Saudi university libraries about cybersecurity and identify the competencies and skills that university librarians must have to achieve cybersecurity requirements from their point of view.

This is done by answering the following questions:

A. Questions

The present study attempted to answer the following questions:

1) What is the degree of cybersecurity awareness among information specialists at Saudi universities' libraries?
2) What are the competencies and skills that information specialists at Saudi universities and libraries must have to keep pace with achieving cybersecurity requirements in Saudi universities' libraries?
3) What are the requirements to achieve cybersecurity from the point of view of information specialists at Saudi universities' libraries?
4) What is the degree of importance of the scientific competencies and skills that information specialists at Saudi universities' libraries must have to achieve cybersecurity requirements from their point of view?
5) What is the degree of training needs required to possess a set of cybersecurity competencies in universities' libraries?
6) Are there any statistically significant differences in the degree of required training to possess the competencies of cybersecurity requirements due to gender, experience, and training courses in computing digital libraries?

B. Aim:

1) To identify the degree of awareness of the nature of cybersecurity among information specialists at Saudi universities' libraries
2) Determining the cybersecurity competencies required for librarians in Saudi universities
3) Determining the most important training needs for information specialists at Saudi universities' libraries to achieve cybersecurity requirements
4) Identifying the significance of the statistical differences in cybersecurity awareness among librarians in Saudi universities according to gender, years of experience, and training courses

IV. MATERIALS AND METHODS

The researcher relied on the descriptive survey method, collecting data about a particular phenomenon and analyzing this data to obtain the study results in which the survey was employed, where the associated variables are used as they are found in nature. So, this study adopted a quantitative approach to achieve the goals mentioned beforehand. According to [29], this approach was appropriate for such a study. this approach was appropriate for such a study.

The questionnaire had six sections: the first section was about demographics. Its purpose was to segment data and draw comparisons within the population, and its three questions specified gender, age, and level of education.

The second section contained phrases measuring cybersecurity awareness, the second section measured cybersecurity competencies, the fourth measured the awareness of cybersecurity systems and methods, the fifth section covered requirements for achieving cybersecurity, and the final section was about cybersecurity needs and risk analysis and assessment.

A. The Sample

The study sample comprised 200 information specialists in Saudi universities during the first semester of the academic year 2022-2023. Random sampling was used to select the participants since it is difficult, if not impossible, to list all members of a target population and choose a sample representing them [30]. The participants were distributed according to gender, experience, and number of training courses in cybersecurity, as shown in Table 1.

Table 1. Distribution of research samples to taxonomic variables

S	Taxonomic variables		Number	Percentage
1	Gender	Male	56	28 %
		Female	144	72 %
Total			200	100 %
2	Experience	Less than 5 years	3	1.5 %
		5 to 10 years	23	11.5 %
		More than 10 years	174	87 %
Total			200	100 %
3	Number of training courses in cybersecurity	No courses in cybersecurity	134	67 %
		Two courses or less	55	27.5 %
		More than 3 courses	11	5.5 %
Total			200	100 %

Table 1 shows that the number of females (72%) participating in this study exceeded males (28%). The percentages of years of experience in the participants' responses were as follows: less than five years, 1.5%; from 5 to 10 years, 11.5%; more than 10 years, 87%.

Based on the participants' responses, 5.5% had more than three courses, 27.5% had two or fewer training courses, and 67% had no courses in cybersecurity.

B. Factorial Validity

Lisrel 8.8 software was used to perform the confirmatory factor analysis for the structure of training needs. The unweighted least square method was used to test the structural validity. The goodness of fit indices was as follows (Table 2):

Table 2. Goodness of fit of the model structure

Index	RMSEA	X2	NNFI	GFI	AGFI
Value	.027	77.79	1	.99	.96

The model was fitting, but the chi-square index was significant because the multivariate normality was violated. The factor loadings were as follows (Table 3):

Table 3. Factor loadings of structure validity

Factor	Factor Loadings	Std Error	t-Value
The cybersecurity competencies	.85	.054	15.63
Awareness of cybersecurity	.71	.050	14.24
Administrative requirements	.69	.049	13.96
Technical requirements	.73	.051	14.38
Physical Requirements	.78	.052	15.06

The factor loadings were within .69–.85. The loadings were satisfied and accepted. RESULTS:

C. Results

To answer the first question, the frequencies and percentages of the tests performed for satisfying cybersecurity awareness among information specialists in Saudi universities are in Table 4 and Table 5.

Table 4. Awareness of cybersecurity levels among information specialists at Saudi universities' libraries

No.	Items	Strongly disagree	Disagree	Undecided	Agree	Strongly agree
1	I have a familiarity with the concept of cybersecurity.	12 6%	12 6%	115 57.5%	49 24.5%	12 6%
2	I am fully aware of the dangers of downloading programs and files from the Internet.	6 3%	2 1%	40 20%	96 48%	56 28%
3	I am aware of the dangers of opening emails from unknown senders, especially if there is an attachment.	1 .5%	5 2.5%	21 10.5%	85 42.5%	88 44%
4	I know the concept of social engineering.	12 6%	49 24.5%	101 50.5%	23 11.5%	15 7.5%
5	I know the dangers of smartphone viruses.	6 3%	6 3%	51 25.5%	73 36.3%	64 32%
6	I know phishing terminology.	7 3.5%	8 4%	57 28.5%	67 33.5%	61 30.5%
7	I feel my organization's computer is safe.	2 1%	7 3.5%	71 35.5%	67 33.5%	53 26.5%
8	I will ensure that if I remove a file from my computer or USB device, the information may be recovered.	3 1.5%	8 4%	76 38%	70 35%	43 21.5%
9	I utilize the same password for my personal and professional accounts.	20 10%	88 44%	47 23.5%	30 15%	15 7.5%
10	I don't share my work password.	--	7 3.5%	34 17%	44 22%	115 57.5%

Table 4 shows that more than half of the participants agree on familiarity with the concept of cybersecurity, but it was noted that the range of the degree from severe to moderate understanding, is represented by about three-quarters of the sample.

Awareness of cyber actions is also high, and this appears in the high percentages of items no. 10 "not sharing passwords" and no. 3, which relates to not opening attachments from unknown persons. The sample reserve is one of the traditional procedures linked to using the same password for more than one personal account for the same person, which is evident from item no. 9. The weighted average of the degrees of cyber awareness among librarians reached the value of 3.66, which is close to the approval limit, which means there is a high degree of relative awareness among the sample.

The next group of questions in the survey is related to the degree of awareness of cybersecurity systems and methods for information specialists in Saudi university libraries (the ability-based approach).

Table 5. Awareness of cybersecurity levels among systems and methods for information specialists in Saudi university libraries (the ability-based approach)

No.	**Items**	Strongly disagree	Disagree	Undecided	Agree	Strongly agree
1	Use an antivirus program regularly	1 .5%	6 3%	32 16%	87 43.5%	74 37%
2	I update my antivirus software regularly.	1 .5%	6 3%	46 23%	79 39.5%	68 34%
3	I am permitted to view only the websites specified by the policy.	6 3%	10 5%	61 30.5%	85 42.5%	38 19%
4	I use an antivirus program regularly.	6 3%	28 14%	72 36%	60 30%	34 17%
5	I have an awareness of knowing what kind of malware it is and installing it on my computer at work.	12 6%	69 34.5%	81 40.5%	18 9%	20 10%
6	I take information security training courses in my workplace	12 6%	65 32.5%	54 27%	37 18.5%	32 16%
7	My computer is of no value to hackers; they don't target me.	10 5%	28 14%	78 39%	48 24%	36 18%
8	Understand what to do if my computer becomes infected with a virus.	14 7%	36 18%	84 42%	48 24%	18 9%

According to Table 5, the respondents show that the ability-based approach depends to a large extent on the degree of awareness of librarians to use and update databases about virus resistance. This is evident from the percentages of the first two statements in the second axis, which exceeded 70%. There is an awareness of consent that exceeds half of the sample opinions about the practices of accessing the allowed sites in the third sentence. However, information specialists cannot distinguish the type of malware and may install it on their work computers. This may be due to their need for technical training in the field of software constantly, which raises the efficiency of distinguishing between programs and sites that represent a danger.

To answer the second question, the frequencies and percentages of the test performed were used, and the results are in Table 6.

Table 6. The cybersecurity competencies levels needed for information specialists in Saudi university libraries

No.	**Items**	Strongly disagree	Disagree	Undecided	Agree	Strongly agree
1	Discovering and identifying cyber threats of all kinds.	13 6.5%	35 17.5%	74 37%	61 30.5%	17 8.5%
2	Knowledge of concepts, vocabulary, principles, and practices pertaining to information security and cyberspace.	14 7%	34 17%	83 41.5%	52 26%	17 8.5%
3	Gaining skills to deal with available technologies, tools, and practical methods in information security and cyberspace	14 7%	68 34%	87 43.5%	62 31%	20 10%
4	Identifying user requirements in designing information systems and constructing safe computer networks.	17 8.5%	68 34%	75 37.5%	24 12%	16 8%
5	Demonstrate knowledge of mathematical principles and algorithms for encryption and protection of systems and information	17 8.5%	32 16%	86 43%	45 22.5%	20 10%
6	Identifying user requirements in designing information systems and constructing safe computer networks.	16 8%	48 24%	84 42%	37 18.5%	15 7.5%
7	Determining the time and cost of remedying the damage caused by an attack on an information system or organization	16 8%	51 25.5%	75 37.5%	36 18%	22 11%
8	Assess appropriate tools and techniques to address the damage caused by security breaches	16 8%	14 7%	72 36%	70 35%	28 14%
9	Defining the rules, procedures, and plans required to manage and secure the library's security.	16 8%	18 9%	54 27%	94 47%	18 9%
10	Apply design, development, and management principles in establishing computer networks	14 7%	19 9.5%	77 38.5%	69 34.5%	21 10.5%
11	Use of different network protocols	14 7%	25 12.5%	65 32.5%	69 34.5%	27 13.5%
12	Building secure information systems and computer networks	14 7%	21 10.5%	66 33%	76 38%	23 11.5%
13	Prepare and present technical reports in a coherent and orderly manner, both verbal and written	12 6%	8 4%	71 35.5%	78 39%	31 15.5%
14	Utilization of best practices and standards in information and network security.	11 5.5%	7 3.5%	49 24.5%	100 50%	33 16.5%
15	The digital identity system must comply with all laws and regulations.	12 6%	4 2%	58 29%	81 45.5%	35 17.5%
16	To be aware of the opportunities and risks inherent in the digital environment in front of being present in the digital identity	1 .5%	--	35 17.5%	97 48.5%	67 33.5%
17	An appreciation of the need and commitment to continuous professional development	1 .5%	--	65 32.5%	89 44.5%	45 22.5%
18	Think logically and analytically	2 1%	--	40 20%	106 53%	52 26%
19	The ability to make decisions	1 .5%	1 .5%	48 24%	77 38.5%	73 36.5%
20	Discover problems and work to solve them	1 .5%	--	41 20.5%	95 47.5%	63 31.5%
21	Constantly looking for opportunities to enhance skills and take responsibility in the work environment	1 .5%	6 3%	58 29%	83 41.5%	52 26%
22	Analyze, compare, and assess critically the trustworthiness and dependability of digital data, information, and content sources.	2 1%	--	68 34%	70 35%	60 35%
23	Handle data appropriately and establish good data security practices	19 9.5%	19 9.5%	55 27.5%	65 32.5%	42 21%

The weighted average of the competencies and skills that university librarians must have to keep pace with achieving cybersecurity requirements in Saudi university libraries was 2.31, meaning that the competencies and skills were deemed inadequate.

To answer the third question, the frequencies and percentages of the test performed were used, and the results are in Table 7.

Table 7. The requirements levels to achieve cybersecurity competences

No.	Items	Strongly disagree	Disagree	Undecided	Agree	Strongly agree
First: Administrative requirements						
1	There is a special department for cybersecurity in the university library.	12 6%	3 1.5%	39 19.5%	92 46%	54 27%
2	Activating security policies for the library's information systems	12 6%	9 4.5%	49 24.5%	70 35%	60 30%
3	Apply the necessary administrative procedures to achieve cybersecurity within the library	12 6%	7 3.5%	47 23.5%	70 35%	64 32%
4	Continuously assessing cybersecurity risks in library information systems	12 6%	8 4%	28 14%	82 41%	70 35%
5	Apply cybersecurity requirements to protect library data and information	12 6%	8 4%	36 18%	70 35%	74 37%
6	Library application of cybersecurity requirements management of data and information backup copies in the library	1 .5%	16 8%	59 29.5%	84 42%	40 20%
Second: Technical requirements						
7	The library has security protection systems for technical and computer devices.	1 .5%	11 5.5%	57 28.5%	61 30.5%	70 35%
8	Continuously update computer systems and software	1 .5%	2 1%	58 29%	71 35.5%	68 34%
9	Protect confidential information of information systems for both employees and library users	6 3%	--	55 27.5%	77 38.5%	62 31%
10	Implementing cybersecurity requirements for managing login identities and permissions	7 3.5%	--	55 27.5%	64 32%	74 37%
11	Providing protection programs against viruses, programs, suspicious activities, and malicious software for the library's information systems	2 1%	7 3.5%	26 13%	89 44.5%	76 38%
Third: Physical requirements						
12	Providing a high-level protection system for cybersecurity	9 4.5%	9 4.5%	38 19%	62 31%	83 41.5%
13	Providing library employees with modern and advanced equipment to manage information systems	7 3.5%	1 .5%	48 24%	51 25.5%	93 46.5%
14	Provide periodic and continuous maintenance necessary to achieve cybersecurity	2 1%	1 .5%	39 19.5%	69 34.5%	89 44.5%
15	Providing the necessary technical support for library employees to address urgent problems	1 .5%	7 3.5%	39 19.5%	68 34%	85 42.5%
16	Providing modern programs to provide protection and cybersecurity for information systems in university libraries	6 3%	2 1%	43 21.5%	83 41.5%	66 33%

Table 7 shows that in the field of administrative requirements. The overall response of respondents about the criteria for achieving cybersecurity is summarized in Table 7. Accordingly, continuously assessing cybersecurity risks in library information systems was found to be the most crucial factor in requirements to achieve cybersecurity, followed by "there is a special department for cybersecurity in the university library." The lowest score was for "library application of cybersecurity requirements, management of data, and information backup copies in the library."

Moreover, "providing protection programs against viruses, programs, suspicious activities, and malicious software for the library's information systems" was the most important factor in the technical requirements, followed by "implementing cybersecurity requirements for managing login identities and permissions." The lowest score was for "the library has security protection systems for technical and computer devices." Finally, "providing periodic and continuous maintenance necessary to achieve cybersecurity" was found to be the most essential factor in the physical requirements to achieve cybersecurity, followed by "providing the necessary technical support for library employees to address urgent problems." The lowest score was for "providing a high-level protection system for cybersecurity."

Table 8 aimed to answer research question no. 5. The results are as follows:

Table 8. Frequencies for questionnaire axes such as mean, weighted mean, median, variance, and skewness.

	Axis 1	Axis 2	Axis 3	Axis 4	Axis 6
Mean	36.5900	27.6500	53.2300	27.40	56.2150
Median	37.0000	27.0000	54.0000	28.0000	56.0000
Variance	30.786	30.289	192.620	21.235	135.185
Skewness	-.682	-.313	-.503	-.352	-1.230
Weighted mean	3.66	3.46	2.31	1.71	3.75
Alpha	.799	.840	.967	.964	.985

The weighted average of axis 5 reached the highest value at 3.75, followed by axis 1 at 3.66, indicating degrees of approval. Axis 2 (3.46) indicated neutrality. Axes 3 (2.31) and 4 (1.71) indicated rejection.

It was clear from the contrast values that the third axis (cybersecurity competencies) was the highest possible, as the contrast value was inflated to a high degree, followed by the sixth dimension (cybersecurity needs and risk analysis and assessment). Despite this, the sixth dimension is slightly higher in average degree than the third dimension, which may be because the individual differences between the respondents on the third dimension are higher than those on the sixth dimension despite the higher sample means in the sixth.

It was observed that the value of the variance in the individual differences in the responses was the least possible in the fourth dimension (requirements for achieving cybersecurity), which was close in the first and second dimensions (awareness of what cybersecurity is and awareness of cybersecurity systems and methods).

The degree of verification in the weighted average was as high as possible in the sixth dimension, followed by the first (awareness of what cybersecurity is), then the second (awareness of cybersecurity systems and methods), the third (cybersecurity competencies), and the fourth (requirements for achieving cybersecurity). The verification degrees in the third dimension and the first dimension were close to the degree of agreement. In contrast, in the second dimension, the verification degree was close to a neutral response, and in the third and second dimensions, it was close to the degree of rejection.

Using tiered multiple variance analysis to analyze the effect of the number of courses, gender, and years of experience on training needs, we demonstrate the results in Table 9.

Table 9 aims to answer the question no. 6.

Table 9. The effects of demographic variables on training needs

Effect		Value	F	Hypothesis df	Error df	Sig.
Intercept	Hotelling's Trace	3.652	345.14	2	189	.000
Gender	Hotelling's Trace	.036	3.42	2	189	.035
Experience	Hotelling's Trace	.023	1.06	4	376	.375
No. of courses	Hotelling's Trace	.038	1.76	4	376	.135
Gender * experience	Hotelling's Trace	.037	3.47	2	189	.033
Gender * courses	Hotelling's Trace	.007	.31	4	376	.874
Experience * courses	Hotelling's Trace	.056	5.29	2	189	.006
Gender * experience * courses	Hotelling's Trace	.000	.[b]	.00	2	.

The results demonstrated the effect of gender on training needs to achieve cybersecurity requirements, whereas the number of years of experience and years of experience did not affect the training needs. The following is the analysis of the post hoc comparisons of the levels of the independent variables, as shown in Table 10:

Table10. The post hoc analysis of significant levels of training needs

Source	Dependent variable	Type III sum of squares	df	Mean square	F	Sig.
Corrected model	cyberrisk	1679.461[a]	9	186.60	9.22	.000
	Cyber_Security_Skills	1691.41	9	187.93	4.72	.000
Intercept	cyberrisk	13256.46	1	13256.45	655.51	.000
	Cyber_Security_Skills	23937.41	1	23937.40	601.04	.000
Gender	cyberrisk	98.05	1	98.05	4.84	.029
	Cyber_Security_Skills	38.55	1	38.57	.96	.326
Experience	cyberrisk	68.77	2	34.38	1.70	.185
	Cyber_Security_Skills	157	2	78.50	1.97	.142
Courses	cyberrisk	143.95	2	71.97	3.56	.030
	Cyber_Security_Skills	173.18	2	86.59	2.17	.117
Gender * experience	cyberrisk	132.20	1	132.20	6.53	.011
	Cyber_Security_Skills	116.61	1	116.61	2.92	.089
Gender * courses	cyberrisk	16.85	2	8.42	.42	.660
	Cyber_Security_Skills	43.39	2	21.70	.54	.581
Experience * courses	cyberrisk	153.59	1	153.59	7.59	.006
	Cyber_Security_Skills	62.49	1	62.49	1.56	.212
Gender * experience * courses	cyberrisk	.000	0	.	.	.
	Cyber_Security_Skills	.000	0	.	.	.
Error	cyberrisk	3842.41	190	20.22		
	Cyber_Security_Skills	7566.97	190	39.82		
Total	cyberrisk	121925	200			
	Cyber_Security_Skills	215212	200			
Corrected total	cyberrisk	5521.87	199			
	Cyber_Security_Skills	9258.38	199			

Gender and the number of courses influenced training needs related to analyzing and evaluating cyber risks in university libraries. The post hoc analysis of gender effects on training needs is presented in Table 11.

Table 11. The post hoc analysis of gender effects on training needs

Dependent variable	Gender	Mean	Std. error	95% confidence interval	
				Lower bound	Upper bound
Cyber risk	male	24.41	1.27	21.90	26.93
	female	22.01	.72	20.59	23.43
Cyber_Security_Skills	male	31.81	1.78	28.28	35.34
	female	30.47	1.01	28.47	32.46

Males outperformed females in the training needs related to the analysis and evaluation of cyber risks. In comparison, the differences in the other dependent variable were very close and insignificant. The post hoc analysis of experience level's effect on training needs is presented in Table 12.

Table 12. The post hoc analysis of experience levels' effect on training needs

Dependent variable	Courses	Mean	Std. Error	95% confidence interval	
				Lower bound	Upper bound
Cyber risk	No courses in cyber-security	22.47	.62	21.23	23.71
	Two courses or less than	25.32	.96	23.41	27.22
	more than 3	21.28	1.82	17.69	24.87
Cyber_Security_Skills	No courses in cyber-security	29.97	.88	28.23	31.71
	two courses or less than	34	1.35	31.33	36.67
	more than 3	29.381[a]	2.556	24.339	34.422

The results were statistically significant in terms of dimensional comparisons of the training needs associated with the analysis and evaluation of electronic risks. The results were superior in terms of "the number of courses less than 2" (25.23). However, the results of librarians with more than 3 courses were the least possible compared to their counterparts who did not receive any training courses. This means that the courses for this category may not correlate to the required job performance or that they are theoretical courses or address more specialized requirements and require further explanation.

V. Discussion

Libraries and information professionals face challenges in keeping pace with the emerging threats in cyberspace as the technological revolution and the emergence of the information society generate many possibilities and areas of work in cyberspace. The development in cyberspace makes it necessary to ensure the security of operations carried out in university libraries. One of the conditions for effective performance is having sufficient knowledge, awareness, and appropriate skills to face any potential threats.

This study aimed to identify the degree of awareness of the nature of cybersecurity among information specialists in Saudi university libraries to determine the required cybersecurity competencies and the most important training needs needed from their point of view, besides identifying the existence of statistically significant differences in cybersecurity awareness among information specialists according to gender, years of experience, and the number of training courses. The results of the first question showed a high degree of relative awareness among information specialists in Saudi university libraries about the nature of cybersecurity.

The results agree with those of [15,16] in that the success of libraries and information facilities in universities depends largely on the qualification of their employees and their full awareness of cybersecurity challenges. Also, those working in this type of library must be competent to carry out their various tasks.

Furthermore, there are training needs that necessitate developing the ability to analyze and identify the risks associated with the information security system in the library, identify opportunities to address risks and define the objectives of the information security system and the plans necessary to achieve them by placing the required resources to build a system that guarantees the confidentiality and protection of information.

Also, the following needs to be addressed: how to plan operating operations to manage the information security system in the university library and set controls to monitor, measure, and evaluate the information security system of the library and how to assess the need for training in preparing an internal audit program and using it to evaluate the information security system.

The results also indicate the importance of training on analyzing and evaluating cyber risks in university libraries; collecting and organizing electronic risk information; identifying, analyzing, and prioritizing information security risks; improving vulnerability management activities by presenting them in the context of risks; managing operational risks in university libraries; developing risk response strategies. Appropriate library business requirements, tools, and applications are required to assess and manage risks to the university library information infrastructure, identify and implement security controls that meet the requirements of managing the university library, implement acceptable security and protection during the system life cycle, and finally provide training on cloud solutions for security and protection.

The study results also demonstrated the need to raise the competencies and skills of the information specialist to keep pace with cybersecurity requirements.

These results differ from those by [27], which revealed teachers' low awareness of cybersecurity and their use of methods and strategies to protect students from the dangers of the Internet

A. Limitations

This search had three limitations, as follows. The study was conducted on a relatively small sample (200) of information specialists in Saudi universities. It was carried out during the academic year 2022/2023. It was carried out in Saudi Arabia, where we evaluated cybersecurity awareness and requirements of competencies and skills to achieve cybersecurity. Therefore, while generalizing the results, these constraints must be considered.

VI. Conclusion

Cybersecurity has become an integral part of the technical system because it protects data, networks, and digital programs and guards against electronic attacks or manipulation of digital data.

The protection and security of information have become an urgent necessity for individuals and institutions to protect knowledge from piracy. Cybersecurity is a global necessity with the spread of technical means for processing, storing,

circulating, and interacting with data via the Internet and information networks.

The issue of cybersecurity in university libraries in the Kingdom of Saudi Arabia is an issue that requires serious administrative and strategic attention. Cybersecurity is hindered due to its financial and social burdens.

The growing number of cyberattacks that exploit the vulnerability of the human factor determines the need to raise efficiencies in the field of cybersecurity. Increasing the knowledge and competencies of information specialists is essential to improving cybersecurity.

REFERENCES

[1] Appiah-Otoo, I., & Song, N. (2021). The impact of ICT on economic growth-Comparing rich and poor countries. Telecommunications Policy, 45(2), 102082.

[2] Vu, K., Hanafizadeh, P., & Bohlin, E. (2020). ICT as a driver of economic growth: A survey of the literature and directions for future research. Telecommunications Policy, 44(2), 101922..

[3] Mitomo, H., Fuke, H., & Bohlin, E. (Eds.). (2015). The smart revolution towards the sustainable digital society: Beyond the era of convergence. Edward Elgar Publishing.

[4] Enisa, M. E. D. E., & Gunes, G. (2019). Integration of intercultural communicative competence (ICC) in an EFL course: Perceptions of students and teachers. İnönü Üniversitesi Eğitim Fakültesi Dergisi, 20(2), 352-363.

[5] Bruggemann, R., Koppatz, P., Scholl, M., & Schuktomow, R. (2022). Global cybersecurity index (GCI) and the role of its 5 pillars. Social Indicators Research, 1-19.

[6] Almomani, I., Ahmed, M., & Maglaras, L. (2021). Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia. PeerJ Computer Science, 7, e703.

[7] Kortjan, N., & Von Solms, R. (2013). A cyber security awareness and education framework for South Africa (Doctoral dissertation, Nelson Mandela Metropolitan University).

[8] Abe, S., Fujimoto, M., Horata, S., Uchida, Y. and Mitsunaga, T. (2016), "Security threats of internet-reachable industrial control system (ICS)", in Society of Instrument and Control Engineers of Japan (SICE) Annual Conference 2016, IEEE Xplore,Tsukuba, pp. 750-755, doi: 10.1109/SICE.2016.7749239

[9] Hassounah, M., Raheel, H., & Alhefzi, M. (2020). Digital response during the COVID-19 pandemic in Saudi Arabia. Journal of medical Internet research, 22(9), e19338.

[10] Renaud, K., & Ophoff, J. (2021). A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. Organizational Cybersecurity Journal: Practice, Process and People.

[11] Nedyalkova, A., Bakardjieva, T., & Nedyalkov, K. (2016). Application of Digital Cybersecurity Approaches to University Management--Vfu Smart Student. International Association for Development of the Information Society.

[12] Ranga, M., & Etzkowitz, H. (2013). Triple Helix systems: an analytical framework for innovation policy and practice in the Knowledge Society. Industry and higher education, 27(4), 237-262.

[13] Al-Khalifa, H. S., Baazeem, I., & Alamer, R. (2017). Revisiting the accessibility of Saudi Arabia government websites. Universal Access in the Information Society, 16, 1027-1039.

[14] Al-Sanea, N. O. (2020) Teachers' awareness of cybersecurity and methods of protecting students from the dangers of the Internet and promoting their national values and identity, Scientific Journal of the Faculty of Education, Assiut University, 26 (6), 40-91

[15] Al-Omran, H. I. (2010). Basic competencies required for information specialists to work in the second generation of information institutions. Journal of King Fahd National Library, 16(1), 5-38.

[16] Al-Harbi, p. H., Al-Azmy, I. R., & Bawaraki, H. c. (2022). Identifying the level of information awareness among library and information science students at the College of Basic Education in the State of Kuwait. Journal of Information Studies and Technology, 2022(2), 10.

[17] Kizza, J. M., Kizza, W., & Wheeler. (2013). Guide to computer network security.

[18] Adakawa, M. I., & Garba, K. D. (2020). Mixed Methodology: Implications For Library And Information Science Research. International Journal of Business Review and Entrepreneurship, 1(1), 55-66.

[19] Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. Journal of Big data, 7(1), 1-29.

[20] Al-Alawi, A. I., & Al-Bassam, S. A. (2019). Evaluation of telecommunications regulatory practice in the Kingdom of Bahrain: development and challenges. International Journal of Business Information Systems, 31(2), 282-303.

[21] Akgün, Ö., & Topal, M. (2015). Information security awareness of senior students of education faculty: Sakarya university education faculty example. Sakarya University Journal of Education, 5(2), 98-121.

[22] Kam, H. J., Ormond, D. K., Menard, P., & Crossler, R. E. (2022). That's interesting: An examination of interest theory and self-determination in organisational cybersecurity training. Information Systems Journal.

[23] San Nicolas-Rocca, T., & Burkhard, R. J. (2019). Information Security in Libraries. Information Technology and Libraries, 38(2), 58-71.

[24] Yiğit, M. F., & Seferoğlu, S. S. (2019). Examination of students' cyber security behaviors according to five factor personality traits and various other variables. Journal of Mersin University Faculty of Education, 15(1), 186-215.
[25] Al Masoud, A. Y. (2020). Cybersecurity and its Mechanisms in Reducing the Deviant Behaviors of Juveniles in the Kingdom of Saudi Arabia: An Analytical Theoretical Study. Journal of the Faculty of Education - Kafrelsheikh University, 20 (4), 411-434
[26] Abeer M. (2019). Students' addiction to using social networking sites and its relationship to psychological security and involvement in cybercrime. International Journal of Educational and Psychological Studies, i(a), 267-293
[27] AL-sahafi, A. H. & Sana, S. (2020). The level of cybersecurity awareness among secondary school computer teachers in Jeddah, Journal of Scientific Research in Education, 20 (10), 493-534
[28] Al-Ghadyan, S., Yahya M., and Ezz Al-Din, A (2018). Pictures of electronic blackmail crimes, their motives, and the psychological effects of them from the point of view of teachers, staff members and psychological counselors. Journal of Security Research: King Fahd Security College - Research and Studies Center, 27 (69), 157-227
[29] Anderson, O., Brodie, A., Vincent, C. A., & Hanna, G. B. (2012). A systematic proactive risk assessment of hazards in surgical wards: a quantitative study. Annals of surgery, 255(6), 1086-1092.
[30] Gates, H. R., Johnson, D. M., & Shoulders, C. W. (2018). Instrument Validity in Manuscripts Published in the" Journal of Agricultural Education" between 2007 and 2016. Journal of Agricultural Education, 59(3), 185-197.

Contribution of individual authors to the creation of a scientific article (ghostwriting policy)

I confirm that I am the only Author of this article that has conducted this study (study's design, data collection, analysis, interpretation, manuscript writing etc.)

Sources of funding for research presented in a scientific article or scientific article itself

No funding was received for conducting this study.

Conflict of Interest

The author declares that they have no conflicts of interest. The funders played no role in the study's design, data collection, analysis, interpretation, manuscript writing, or decision to publish the findings.

Ethical Approval

All procedures performed in the study followed the ethical standards of the institutional research committee of the Deanship of Scientific Research at the Princess Nourah bint Abdulrahman University with the 1964 Helsinki declaration and its later amendments.

Data Availability Statement

The raw data supporting the conclusion of this article will be available upon request to the corresponding author