International Journal of Instruction *October 2023 ● Vol.16, No.4*
e-ISSN: 1308-1470 ● www.e-iji.net *p-ISSN: 1694-609X*
pp. 173-188

Article submission code: 20221021140341
Received: 21/10/2022
Revision: 17/03/2023
Accepted: 09/04/2023
OnlineFirst: 10/07/2023

The Cybersecurity Practice in Saudi Universities to Protect the Intellectual Rights of Faculty Members' Publications

Wedad Abdullah Nasser Sharabi
Department of Educational Sciences, College of Education in Al-Dilam, Prince Sattam bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia, W.*_smarty@hotmail.com*

This study aimed to identify the reality of cybersecurity practice in Saudi universities to protect the intellectual rights of faculty members' publications. The study population consisted of all faculty members at Taif University, Umm Al-Qura University, King Abdulaziz University, and Prince Sattam bin Abdulaziz University. Participants were 120 faculty members from the four universities. The descriptive-analytical method was used and data was collected by a questionnaire developed by the author. The results revealed that cybersecurity practice in Saudi universities for protecting the intellectual rights of faculty members' publications is high. Obstacles to cybersecurity practice in Saudi universities are medium. Ways to overcome obstacles to cybersecurity practice in Saudi universities are high. No statistically significant differences (p=0.05) were found in the views of the participants in the questionnaire's individual dimensions or the total score by gender, experience, academic rank, and university. Based on the study results, it is recommended that universities reduce the obstacles to cybersecurity practice reported by the participating faculty members and put the ways they proposed into practice to take the cybersecurity practice to a higher level.

Keywords: cybersecurity, practice, intellectual property rights, faculty members, Saudi universities

INTRODUCTION

Society, economy and critical infrastructures now depend on computer networks and information technology. Cyber-attacks have become more prevalent and potentially more catastrophic with the ever-increasing dependence on information technology. Cybersecurity is concerned with understanding the issues surrounding cyber-attacks and devising defensive strategies (i.e., countermeasures) that maintain the confidentiality, integrity, and availability of any digital and information technologies.

The Kingdom of Saudi Arabia's Vision 2030 and the Digital Transformation Program 2020 stress the importance of expanding electronic use in governmental, scientific and commercial work, which also emphasizes the importance of cybersecurity. For this reason, The Kingdom has established the Cybersecurity Authority which is linked to the

Citation: Sharabi, W. A. N. (2023). The Cybersecurity practice in Saudi universities to protect the intellectual rights of faculty members' publications. *International Journal of Instruction*, *16*(4), 173-188. https://doi.org/10.29333/iji.2023.16411a

highest authority in the government, i.e., the Custodian of the Two Holy Mosques. Many global and local reports, e.g., the report of the Norton Company have indicated that Saudi institutions, including educational institutions have been exposed to many cyber-attacks. The report stated that 85% of the Kingdom's population was subjected to cyber-attacks, a percentage which is 10% higher than the global percentage (Abu Zaid, 2019).

Cyberspace is an area through which the security of countries can be threatened. Therefore, the more countries possess defensive strategies and tools, the more they can achieve their cybersecurity that complements their national sovereignty (Kalaa, 2022). The importance of deterring cybersecurity risks is particularly evident in institutions whose work relies primarily on knowledge resources, especially educational and academic institutions like higher education institutions. These institutions have their own unique knowledge assets that must be protected, e.g., courses and research production of faculty members. Therefore, it is important to have cybersecurity measures in place in order to guarantee the protection of those assets.

Educational opportunities resulting from technological development have raised new challenges for intellectual rights protection laws in higher education. Faculty members have become more alert to changing trends in intellectual rights protection. The scope of intellectual property typically includes inventions or discoveries that are protectable by patents, trademarks, and copyrights (Kang, et al., 2020). The protection of the knowledge assets of universities and the intellectual property rights of research products is as important as the intellectual property of companies. It is therefore of paramount importance to take the appropriate measures, particularly cybersecurity measures to protect the intellectual property rights of universities and the publications of faculty members from attacks and violations committed mainly in the cyberspace.

Accordingly, it is crucial to educate faculty members, university administrations, and higher education institutions about cybersecurity. There is a need to effectively apply cybersecurity in these institutions to protect the intellectual property rights of faculty members' publications from the dangers of the Internet, cyber-attacks and hacking attempts.

Objectives and Study Questions

A feature that characterizes the contemporary world is the widespread use of information and communication technologies in all fields of life and most notably in higher education. The reason for this is that these technologies with the potential of cyberspace can perform activities more easily. However, these technologies have also facilitated criminal and illegal actions, including cybersecurity threats. Perhaps the most prominent cybersecurity threats that cause great damage in higher education are those that target the violation of intellectual property rights of faculty members' publications. This problem is now threatening information security in higher education institutions. Several previous studies (Ibn Ibrahim, 2021; Al-Manea, 2022) have shown that there is a wide consensus on the need to achieve cybersecurity requirements in Saudi universities. Thus, the current study aimed to explore the role of cybersecurity practice in Saudi universities in protecting the intellectual rights of faculty members' publications. More specifically, the study attempted the following questions:

1. What is the reality of cybersecurity practice in Saudi universities to protect the intellectual rights of faculty members' publications?
2. What are the obstacles to cybersecurity practice in Saudi universities to protect the intellectual rights of faculty members' publications?
3. What are the ways to overcome the obstacles to cybersecurity practice in Saudi universities to protect the intellectual rights of faculty members' publications?
4. Are there significant differences in the participants' responses to the questionnaire's dimensions by gender, experience, academic rank, and university?

Review of Literature

The Importance of Cybersecurity

Universities and academic institutions have become prominent targets of cyber-attacks, and many universities have already suffered from several high-impact incidents. Universities and academic institutions manage large amounts of knowledge resources like policies, courses, programs, research products and personal data, which make universities an attractive target for cybercriminals, spyware, and hacking activists.

Human factors are the weakest elements in cybersecurity today and higher education institutions. Thus it is crucial to build a cybersecurity culture to change attitudes and perceptions and inculcate good security behaviors in universities. Good cybersecurity practice is also critical to support the smooth achievement of security-related plans and policies in universities (Cheng & Wang, 2022). Al-Samhan (2020) asserts that today's world is interconnected by networks and everyone benefits from cyber defense programs. She identified the importance of cybersecurity for contemporary universities as follows:

- Maintaining the integrity of universities' knowledge resources and achieving an abundance of data.
- Protecting devices and networks as a whole from intrusions targeting educational polices and materials.
- Detecting and addressing weaknesses in educational electronic systems.
- Using open knowledge resources tools to achieve cybersecurity.
- Providing a safe work environment via the Internet.

Aims of Cybersecurity in Saudi Universities

Cybersecurity seeks to protect computer networks and the information they contain from intrusion, damage or malicious disruption. It reduces the risk of malicious attacks on electronic educational systems, including programs, computers, and networks, using tools that detect intrusions, stop viruses, block malicious access, enforce identity examination, enable encrypted communications, etc. The aims of cybersecurity policies in universities are to produce more secure tools and systems, enhance security preventive behaviors, and effectively manage persistent vulnerabilities that arise from the ever-changing cyber threats (Sedenberg & Mulligan, 2015). Cyber security in Saudi universities aims to (Al-Shammari & Ismail, 2020):

- Resolve and recover from cyber incidents and attacks, through timely circulation of educational and research material, cooperation and taking necessary actions.
- Establish a mechanism to manage the treatment of electronic incidents.
- Establish a network for exchanging educational and research material among cybersecurity operation centers to facilitate dealing with incidents, exchange information and provide training opportunities.
- Reduce the vulnerability of the universities' information infrastructure to electronic attacks.

Intellectual Property

Intellectual property is intangible and legally recognized. The Intellectual property law allows creators of ideas and inventions to prevent other entities from using them without permission. The main components of intellectual property are patents, copyrights, trademarks, and other legal forms of intellectual property. The creative intellectual practice is one of the noblest human practices. From these practices the cultures of nations are crystallized and civilizations are built. The intellectual right comes at the top of all rights. If material productions constitute an important element in the building and progress of nations, intellectual productions are no less important (Van Norman & Eisenkot, 2017). Of course, faculty members' intellectual productions need to be protected by laws and cybersecurity. This is an important role to be played by modern universities.

The need for international protection of intellectual property has become urgent. What fueled that need was the reluctance of exhibition owners to participate in the World Exhibition of Inventions that was held in Vienna in 1873 for fear of theft of their ideas. Documents indicate that the year 1883 witnessed the birth of the "Paris Convention for the Protection of Industrial Property", which is the major international treaty aimed at helping the citizens of a country to obtain protection for their intellectual creations in other countries. In 1886, copyright entered the international arena through the Berne Convention for the Protection of Literary and Artistic Works. The aim was to help citizens of its member states to control their innovative work (Fatoum, 2020). The use of copyright as a tool for preserving creative work has recently gained great momentum, as the advent of ICTs in recent years has increased the importance of copyright protection (Brem, et al., 2017).

Patents, many of which are created in universities, are commonly used to protect technological innovations or innovative processes. A patent is granted for a limited period, usually twenty years, and gives the patentee a set of rights including the right to exclude others from duplicating, using or selling patented intellectual property. In return, the patentee discloses information about the patented technology. The primary purpose of the patent is to support innovation (Raiser, et al., 2017). The terms of the patent stipulate (Al-Noor, 2020) that the invention must be new, viable industrially, and legitimate.

The Role of Cybersecurity in Protecting the Intellectual Property of Faculty Members in Saudi Universities

Internet crimes are an emerging criminal phenomenon. The French jurist Miller alerted to the danger of the misuse of the computer stating that the computer with its greed for collecting information, accuracy, and capacity to recall whatever is stored in it may turn our lives upside down (Taha, 2012). Securing the cyberspace of universities is a challenging task that requires well-educated and trained professionals. Preparing personnel who can monitor and ensure the security of the cyberspace of universities has become urgent. Accordingly, the development of effective cybersecurity programs is gaining more emphasis in the academic and university community (Zarour, et al., 2020).

Universities must learn from previous hacking incidents in higher education services and be always prepared to protect themselves from all potential attacks that might target their computer-based digital systems. Universities should therefore improve security at all levels: technical, physical, and administrative. This is important because if the platforms used in universities are not secure, the intellectual property rights of faculty members and instructional materials may not be secure (Almomani, et al., 2012).

Cybersecurity protects the intellectual property of faculty members by educating users about the proper use of electronic resources, preventing illegal use of libraries, stopping infringing activities, protecting the privacy of faculty members and users, respecting licenses, and providing access to licensed information at reasonable prices (Nasser, 2018). There are two ways for cybersecurity to maintain the intellectual property rights of faculty members (Abdul Rahman, 2021):

- Protection of digital works through legal protection that depends on warning before use and punishment after misuse.
- Technical protection which is prevalent in most developing countries. This type of protection depends on setting technical obstacles that prevent misuse, e.g., setting passwords and encrypting work.

Previous Studies

Al-Manea (2022) explored the reality, requirements, and obstacles to achieving cybersecurity in Saudi universities in the light of the 2030 Vision. A cohort of 210 technical employees in three Saudi universities: Umm Al-Qura University, Imam Abdulrahman bin Faisal University, and Imam Muhammad bin Saud Islamic University responded to a questionnaire probing the reality, requirements, and obstacles to achieving cybersecurity in Saudi universities. The results revealed that the most important obstacles to achieving cybersecurity in Saudi universities were the low level of expertise of the employees and the weak cooperation among technology employees in the universities. The majority of the participants agreed that cybersecurity in Saudi universities needs to be promoted. Ibn Ibrahim (2021) developed a scale to measure elementary school science teachers' (N=30) awareness of the aspects of cybersecurity in distance education. A proposed training program targeting aspects of cybersecurity in distance education was then taught to participants. The results revealed the need for promoting awareness of cybersecurity in Saudi educational institutions.

Al-Bishi (2021) investigated the reality of cybersecurity in Saudi universities and its impact on enhancing the digital culture from the perspective of faculty members. A cohort of 182 faculty members responded to a questionnaire developed by the author to collect the required data. The results revealed that the level of cybersecurity in Saudi universities was high (73.18%) and so was the level of digital culture (74.58%). Al-Qahtani (2019) explored Saudi university students' (N=486) of cybersecurity: its concept, the most important crimes it deals with, ways of prevention from cyberspace crimes, and obstacles to prevention from these cyberspace crimes. The participants viewed cybersecurity as the use of a set of technical, organizational and administrative means to prevent unauthorized use of electronic transactions and communication and information systems.

Miro and Amparado (2019) assessed faculty members' knowledge of intellectual property and their rights. A cohort of 102 faculty members from the Universities of Cebu and Mandaue in the Philippines participated in the study. The results revealed that faculty members' knowledge of copyrights, patents and trademarks was medium. Tinao et al. (2018) investigated the attitudes, awareness and aspirations of intellectual property among students and faculty members in universities. A cohort of 124 students and faculty members from the Bataan Peninsula State University in the Philippines participated in the study. Data collection methods included a questionnaire, personal interviews and focus groups. The results revealed that knowing where to find and use patent information is the most important topic in the study of intellectual property from the perspective of students and faculty members. A positive relationship was found between improving the services, processing and application of intellectual property and enhancing the efficiency of the intellectual property system at the university.

METHOD

The study used the descriptive-analytical method, which is "a form of organized scientific analysis and interpretation to describe a specific phenomenon or problem and depict it quantitatively by collecting data and specific information about it" (Abdul-Moumen, 2008).

The Participants

The study population was faculty members at Taif University, Umm Al-Qura University, King Abdulaziz University, and Prince Sattam bin Abdulaziz University. The first three universities and the fourth university where I work were chosen because they are located in the western region of the Kingdom of Saudi Arabia. The proximity of the universities would make it easier to recruit respondents. Furthermore, the four universities are among the Saudi universities that have applied cybersecurity. The data collection instrument was electronically sent to faculty members in the four universities via e-mails and WhatsApp. A total of 120 faculty members (68 males, i.e., 56.7% and 52 females, i.e., 43.3%) completed the questionnaire. They varied in their teaching experience and academic rank. Table 1 presents the characteristics of the participants.

Table 1
Characteristics of the participants

Variable		Frequency	%
Experience	< 5 years	9	7.6
	From 5 to < 10 years	84	70
	≥ 10 years	27	22.5
Academic Rank	Assistant professors	67	55.8
	Associate professors	27	22.5
	Professors	26	21.7
University	Taif University	17	14.2
	Prince Sattam University	47	39.2
	King Abdulaziz University	25	20.8
	Umm Al-Qura University	31	25.8

The Instrument

To collect the required data, the author developed a 30-item questionnaire that had three dimensions, 10 items each. The first dimension dealt with the reality of cybersecurity practice in Saudi universities to protect the intellectual rights of faculty members' publications. The second dimension included items tapping the obstacles to cybersecurity practice in Saudi universities. The third dimension dealt with ways to overcome the obstacles to cybersecurity practice in Saudi universities. Items were answered based on a 5-point rating scale ranging from 5 "strongly agree" to 1 "strongly disagree".

To establish the construct validity of the questionnaire, the questionnaire was pilot-tested on 30 faculty members from outside the main study sample. Correlations among items and their respective dimensions were computed. Items correlated with the dimension of the reality of cybersecurity practice in Saudi universities with coefficients ranging between 0.54 and 0.90, with the dimension of the obstacles to cybersecurity practice in Saudi universities with coefficients ranging between 0.56 and 0.84, and with the dimension of the ways to overcome the obstacles to cybersecurity practice in Saudi universities with coefficients ranging between 0.56 and 0.86. All correlation coefficients were significant at the 0.01 level. Additionally, the dimensions significantly (p=0.01) correlated with the questionnaire's total score. More specifically, the reality of cybersecurity practice in Saudi universities, the obstacles to cybersecurity practice in Saudi universities, and ways to overcome the obstacles to cybersecurity practice in Saudi universities correlated with the questionnaire's total score with coefficients of 0.95, 0.95, and 0.96 respectively. The high correlations among items and their respective dimensions and among items and the questionnaire's total score indicate that the questionnaire had good construct validity

As to reliability, the subdimensions of the reality of cybersecurity practice in Saudi universities, the obstacles to cybersecurity practice in Saudi universities, ways to overcome the obstacles to cybersecurity practice in Saudi universities, and the questionnaire as a whole yielded alpha reliability estimates of 0.97, 0.98, 0.96, 0.75, 0.97 respectively. The subdimensions of soft skills, lifelong learning skills, digital skills, and the total future skills dimension yielded alpha reliability estimates of 0.73, 0.71, 0.76, and 0.82, respectively. All alpha reliability estimates were significant at the 0.01 level, hence indicating that the questionnaire was quite reliable.

Data Analysis

To analyze data and answer the research questions, descriptives, the t-test for independent samples and one way analysis of variance were calculated using the SPSS program. Prior to conducting the ANOVA test to investigate differences on the questionnaire dimensions by gender, experience, academic rank, and university, the normal distribution of data was checked using Shapiro-Wilk test. The obtained Shapiro-Wilk values for gender, experience, academic rank, and university were 0.597, 0.555, 0.420, and 0.628 respectively. All obtained values were greater than 0.05, which supports the normal distribution of data.

FINDINGS

The Reality of Cybersecurity Practice, the Obstacles to Cybersecurity Practice and Ways to Overcome the Obstacles to Cybersecurity Practice in Saudi Universities

Table 2
Descriptives of the three dimensions of the questionnaire

Dimension	M	SD	Degree of Agreement
The reality of cybersecurity practice in Saudi universities	4.10	0.71	High
Ways to overcome the obstacles to cybersecurity practice in Saudi universities	3.48	0.71	High
The obstacles to cybersecurity practice in Saudi universities	3.01	0.96	Medium
Total	3.53	0.62	

It is evident from Table 2 that the reality of cybersecurity practice in Saudi universities ranked first with a mean of 4.10, followed by ways to overcome the obstacles to cybersecurity practice (M=3.48), and obstacles to cybersecurity practice (M=3.02). This indicates that the participants are quite satisfied with the reality of cybersecurity in their universities. They strongly agreed with ways offered in the questionnaire to improve cybersecurity in Saudi universities. Nonetheless, their medium rating of the obstacles dimension signifies that some obstacles do exist and need to be addressed (see the appendix for items and their means). Example of obstacles reported with medium ratings are “lack of a clear and binding strategy for those involved in storing and processing information at the university”, “continuous maintenance of software and network systems”, and “Absence of a professional coding system to preserve the publications of faculty members”.

Differences in the Participants' Responses to the Questionnaire by Gender, Experience, Academic Rank, and University

Differences by Gender

Table 3
The t-test for gender differences in responses to the questionnaire

Dimension	Gender	N	M	SD	DF	t-value	Sig.
The reality of cybersecurity practice in Saudi universities	Males	68	4.0	0.75	118	-.49	0.61 (not sig.)
	Females	52	4.1	0.69			
The obstacles to cybersecurity practice in Saudi universities	Males	68	2.9	0.89	118	-.80	0.42 (not sig.)
	Females	52	3.1	1.05			
Ways to overcome the obstacles to cybersecurity practice in Saudi universities	Males	68	3.4	0.62	118	-.69	0.48 (not sig.)
	Females	52	3.5	0.82			
Total	Males	68	3.5	0.55	118	-.87	0.38 (not sig.)
	Females	52	3.6	0.70			

It is evident from data in Table 3 that there were no statistically significant gender differences in the participants' responses to the individual dimensions or the total score. That is, male and female faculty members share the same opinions and aspirations regarding cybersecurity in their universities.

Differences by Experience

Table 4
ANOVA test for the differences in responses to the questionnaire by experience

Dimension		Sum of Squares	DF	MS	F	Sig.
The reality of cybersecurity practice in Saudi universities	Between Groups	0.48	2	0.24	0.46	0.63 (not sig.)
	Within Groups	61.0	117	0.52		
	Total	61.5	119			
The obstacles to cybersecurity practice in Saudi universities	Between Groups	3.35	2	1.67	1.84	0.16 (not sig.)
	Within Groups	106.3	117	0.90		
	Total	109.6	119			
Ways to overcome the obstacles to cybersecurity practice in Saudi universities	Between Groups	5.17	2	2.58	5.49	0.12 (not sig.)
	Within Groups	55.05	117	0.47		
	Total	60.22	119			
Total	Between Groups	1.96	2	0.98	2.62	0.09 (not sig.)
	Within Groups	43.90	117	0.37		
	Total	45.87	119			

Data in Table 4 reveals that there were no statistically significant differences in the participants' responses to the individual dimensions or the total score by experience. This indicates that faculty members have the same views on cybersecurity practice regardless of their years of experience in universities.

Differences by Academic Rank

Table 5
ANOVA test for the differences in responses to the questionnaire by academic rank

Dimension		Sum of Squares	DF	Mean Squares	F	Sig.
The reality of cybersecurity practice in Saudi universities	Between Groups	0.27	2	0.14	0.26	0.76 (not sig.)
	Within Groups	61.25	117	0.52		
	Total	61.53	119			
The obstacles to cybersecurity practice in Saudi universities	Between Groups	0.14	2	0.07	0.08	0.93 (not sig.)
	Within Groups	109.55	117	0.94		
	Total	109.69	119			
Ways to overcome the obstacles to cybersecurity practice in Saudi universities	Between Groups	0.03	2	0.02	0.03	0.97 (not sig.)
	Within Groups	60.19	117	0.51		
	Total	60.22	119			
Total	Between Groups	0.02	2	0.01	0.03	0.97 (not sig.)
	Within Groups	45.84	117	0.39		
	Total	45.87	119			

As shown in Table 5, no statistically significant differences were found in the participants' responses to the individual dimensions or the total score by academic rank. This indicates that faculty members with various academic ranks have the same views on the role of cybersecurity in protecting faculty members' publications. All faculty members publish articles and are aware of the significance of cybersecurity in protecting their scientific production.

Differences by University

Table 6
ANOVA test for the differences in responses to the questionnaire by university

Dimension		Sum of Squares	DF	Mean Squares	F	Sig.
The reality of cybersecurity practice in Saudi universities	Between Groups	0.21	3	0.07	0.13	0.94 (not sig.)
	Within Groups	61.32	116	0.53		
	Total	61.53	119			
The obstacles to cybersecurity practice in Saudi universities	Between Groups	3.16	3	1.06	1.22	0.33 (not sig.)
	Within Groups	106.52	116	0.92		
	Total	109.69	119			
Ways to overcome the obstacles to cybersecurity practice in Saudi universities	Between Groups	1.11	3	0.37	0.73	0.54 (not sig.)
	Within Groups	59.11	116	0.51		
	Total	60.22	119			
Total	Between Groups	1.045	3	0.35	0.90	0.44 (not sig.)
	Within Groups	44.82	116	0.39		
	Total	45.87	119			

It can be seen from data in Table 6 that there were no statistically significant differences in the participants' responses to the individual dimensions or the total score by university. This indicates that all Saudi universities are interested in achieving good levels of cybersecurity.

DISCUSSION

That the reality of cybersecurity practice received high rating from the participating faculty members can be due to the great emphasis that universities place on protecting faculty members' publications. Nowadays, Saudi universities reward faculty members who publish in indexed journals to raise their rank internationally. For this reason, they allocate large material, technical or administrative capabilities to protect the publications of their faculty members. This finding is consistent with the study of Ibn Ibrahim (2021) which reported that the social reality in the Kingdom of Saudi Arabia is concerned with providing cybersecurity awareness and training for all institutions. It also concurs with the findings of Al-Bishi's study (2021) which confirmed that the reality of cybersecurity in Saudi universities from the perspective of faculty members is high. This finding indicates that the protection of knowledge assets in universities, e.g., policies, courses, programs and research products have recently received considerable attention from Saudi universities.

The finding that the obstacles to cybersecurity practice in Saudi universities received a medium rating from the participants may be attributed to the administrative regulations and laws in force in Saudi universities which enhance the protection of the intellectual property rights of faculty members. These regulations reduce obstacles to the protection of intellectual property rights. Saudi universities currently place great emphasis on faculty members' quality scientific production. For this reason, they exert all possible efforts to create a supportive and safe research environment. They therefore respond to any obstacles to cybersecurity once they emerge. This finding is in line with the study of Ibn Ibrahim (2021) which emphasized that Saudi universities have sufficient awareness of cybersecurity. Nonetheless, this finding indicates that some obstacles exist and in this the current study concurs with the study of Al-Manea (2022) which reported a low level of expertise and poor cooperation among technology employees in universities to achieve cybersecurity. It is therefore recommended that universities identify obstacles to cybersecurity from the faculty members' perspective and address them in order to improve their cybersecurity.

The participants' rating of the ways to overcome obstacles to cybersecurity practice was high. This means that they strongly agreed with the ways offered in the questionnaire to overcome obstacles and take the cybersecurity in Saudi universities to a higher level. For instance, they strongly agreed with items "It is essential activate digital identity protection programs based on the electronic signature to ensure the integrity and confidentiality of information" (M=4.20), "It is essential to use and develop open source tools to achieve the principles of cybersecurity" (M=4.12), and "It is essential to hire specialized programmers to protect websites for publishing faculty members' articles" (M=3.80). This finding concurs with other studies where similar recommendations were offered to improve the reality of cybersecurity in Saudi universities (e.g., Al-Manea, 2022).

Lack of gender differences in faculty members' views on cybersecurity in Saudi universities can be due to the fact that both sexes are exposed to the same experiences and are affected by the same environmental factors within universities. They also share the same opinions on ways to improve cybersecurity practice in their universities. This finding agrees the study of Al-Manea (2022) where no statistically significant differences were between the responses of male and female faculty members on cybersecurity practice in universities.

That experience did not affect participants' views on cybersecurity in Saudi universities can be due to the fact that all faculty members are exposed to the same guidelines and regulations of cybersecurity practice and receive the same awareness-raising training. All faculty members with many or few years of experience in Saudi universities are now required to publish at least one article in indexed journals, so their contracts with universities can be renewed. This makes all faculty members concerned with copyrights and cybersecurity. This same finding was reached in the study of Al-Bishi (2021).

The nonsignificant differences in the participants' views by academic rank indicate that all faculty members with different ranks share the same opinions and experience of cybersecurity in their universities. This also indicates that universities involve all faculty members regardless of their rank in their cybersecurity practice. This finding is consistent with the study of Al-Bishi (2021) where the academic rank had no significant effect on the participants' views on similar aspects of cybersecurity.

Finally, no significant differences were found among the four universities in cybersecurity practice. This indicates that Saudi universities are equally interested in cybersecurity. In fact, Saudi universities use similar, if not the same, strategies and mechanisms of cybersecurity to protect their information assets and the intellectual rights of their faculty members' research products. The need to practice cybersecurity in universities is universal given the ever-increasing cyberspace threats to cybersecurity and the intellectual rights. This finding is in line with the study of Al-Manea (2022) where affiliation had no significant effect on faculty members' views on similar aspects of cybersecurity.

CONCLUSION

This paper investigated the reality of cybersecurity applied practices at Saudi universities to protect their information assets and the intellectual property rights of faculty members' publications. However, a limitation that affects the generalizability of findings is that the research was conducted on only four universities. Furthermore, the research sample was not large enough, only 120 faculty members. Similar future investigations should overcome this limitation, so they can reach more generalizable findings. Findings of the current study show that cybersecurity applied practices are commonly implemented at Saudi universities and that such practices are important for protecting the intellectual property of faculty members' research products. Moreover, findings show that sample members' views did not significantly differ by gender, years of experience, academic rank, and university, thereby indicating a general and strong agreement on the current state of cybersecurity applied practices at Saudi universities. The implementation of cybersecurity practices has become a necessity in contemporary higher education institutions. The intersection of factors such as increased research productivity in universities and growing cybersecurity threats resulting from the advancement of information and communication technologies makes universities' information assets and research output under constant threats of cybercrimes. The implementation of proper and adequate cybersecurity measures may be of significant values in deterring the threats of crimes and attacks that target universities' information assets and faculty members' intellectual property rights.

Based on the findings, the study offers the following recommendations:

- Saudi universities should address the obstacles to cybersecurity that the participants reported in the present study.
- Saudi universities should apply the recommendations offered by the participants to improve their cybersecurity practice.
- Saudi universities should establish protocols for cooperation with local and international companies specialized in providing electronic security services to obtain the latest technologies and innovations necessary to protect their information assets.
- Replicating the study on a larger number of universities and a larger sample to reach more generalizable findings.

ACKNOWLEDGMENTS

This research was supported by the Deanship of Scientific Research, PSAU (Prince Sattam bin Abdulaziz University), Al-Kharj, Saudi Arabia, under the research project no. 2022/02/22120

REFERENCES

Abdul-Moumen, A. M. (2008). Research in social sciences. *October 7 University Publications, Department of Publications and Publishing*, Libya.

Abdul-Rahman, F. O. (2021). Technical protection measures to protect copyright on the Internet. *Al-Qolzam J. for Security and Strategic Studies, 5*, 189-212.

Abu Zaid, A. A. (2019). Cybersecurity in the Arab World: A Case Study of the Kingdom of Saudi Arabia. *Political Perspectives, 48,* 55-61.

Al-Bishi, M. (2021). Cybersecurity in Saudi universities and its effect in enhancing digital trust from the viewpoint of faculty members: A study on the University of Bisha. *J. The Islamic University of Educational and Psychological Studies, 29,* 353-372.

Al-Manea, A. I. (2022). Requirements to Achieving Cybersecurity in Saudi Universities in the Light of Vision 2030. *J. Faculty Educ., Assiut University,* 38, 155-194.

Almomani, I, M. & Maglaras, L. (2012). Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia. *PeerJ Computer Science, 7*, 1-26.

Al-Noor, G. M. (2020). Patent rights: their legal nature and legal adaptation. *Amarabak,* 11, 93-106.

Al-Qahtani, N. N. (2019). Availability of cybersecurity awareness among Saudi university students from a social perspective: A field study. *Social Affairs, Sociologists Association in Sharjah, 36*, 85-120.

Al-Samhan, M. A. (2020). Requirements to achieve cybersecurity for management information systems at King Saud University. *J. Faculty Educ., Mansoura University,* 111, 2-29.

Al-Shammari, S. M. & Ismail, Z. M. (2020). Cybersecurity as a new anchor in the Iraqi strategy. *Political Issues J., College of Political Science, Al-Nahrain University, 12*, 273-296.

Brem, A., N. & Hitchen, E. L. (2017). Open innovation and intellectual property rights: How do SMEs benefit from patents, industrial designs, trademarks and copyrights? *Management Design, 55,* 1285-1306.

Cheng, E. C., & Wang, T. (2022). Institutional Strategies for Cybersecurity in Higher Education Institutions. *Information, 13*, 1-14.

Fatoum, G. (2020). *Copyright, intellectual property and related rights in the Arab world and the Middle East*. A Report Issued by the International Federation of Journalists.

Ibn Ibrahim, M. H. (2021). Awareness of the aspects of cybersecurity in distance education. *Scientific J. King Faisal University, Humanities and Administrative Sciences, 22*, 299-307.

Kalaa, S. (2022). Cybersecurity and the challenges of espionage and electronic penetration of countries through cyberspace. *J. Law and Human Sciences*, Zayan Ashour University in Djelfa, *15*, 292-314.

Kang, R. C. & Ke, J. (2020). Faculty Intellectual Property Rights in Distance Learning Courses. *J. Higher Education Theory and Practice, 20,* 55-66.

Miro, A. C. & Amparado, M. A. (2019). Intellectual property: are faculty members aware of their rights? *Cebu J. of Computer Studies, 2*, 1-21.

Nasser, G. K. (2018). *Intellectual property protection: copyrights under national legislation and international agreements.* Unpublished PhD Dissertation, Faculty of Humanities and Islamic Sciences, University of Oran - Ahmed Ben Bella, Algeria.

Raiser, K., H. & Bruhn, T. (2017). Corporatization of the climate? Innovation, intellectual property rights, and patents for climate change mitigation. *Energy Research & Social Science, 27*, 1-8.

Sedenberg, E. M. & Mulligan, D. K. (2015). Public Health as a Model for Cybersecurity Information Sharing. *Berkeley Technology Law J., 30*, 1687-1740.

Taha, M. A. (2012). *The legislative confrontation of computer and internet crimes: A comparative study* (1st Edition). Egypt: Dar Al-Fikr and Al-Lawun for Publishing and Distribution.

Tinao, E. S. & de Jesus, A. O. (2018). *Taking intellectual property rights serious: are we in or out? (Phase 1: intellectual property awareness among students and faculty: tracking changing attitudes and awareness.* A paper presented at the 4th International Research Conference on Higher Education, Grand Ina Bali Resort and Beach Hotel, Bali, Indonesia.

Van Norman, G. A. & Eisenkot, R. (2017). Technology transfer: from the research bench to commercialization: part 1: intellectual property rights - basics of patents and copyrights. *Basic to Translational Science, 2,* 85-97.

Alenezi, M., D. & Alsmadi, I. (2020). Toward effective cybersecurity education in Saudi Arabia. In S. Latifi (Ed.), *Advantages in Intelligent Systems and Computing,* 1134 (pp. 79-85), Cham: Springer.

The Appendix

The Cybersecurity Practice Questionnaire

No.	Statement	M	SD
The reality of cybersecurity practice in Saudi universities			
1	The university's internal rules and regulations are in line with international intellectual property laws.	4.03	.893
2	The university adheres to filing claims under applicable local and international anti-cybercrime laws	4.12	.832
3	The university upholds its right to claim compensation in favor of faculty members for damages resulting from violations of the intellectual property protection of their writings.	4.31	.742
4	The university is keen to constantly register patents and copyrights for faculty	4.31	.960

	members.		
5	The University recognizes the importance of teaching staff members about safe surfing on the Internet.	3.93	1.06
6	The university respects intellectual property rights and applies their laws.	4.09	.970
7	The university is interested to hire programmers to protect the cyberspace of its website and platforms for displaying the publications of its faculty members.	3.98	.944
8	The University intellectual property protection laws regulate the use of electronic resources by faculty members.	4.12	.972
9	The university legislates Intellectual property protection laws so that they are sufficient and do not need development.	4.10	.965
10	There is a legal framework regulating intellectual property in the university.	4.09	1.00
	Total	4.11	.7191
Obstacles to cybersecurity practice in Saudi universities			
11	Using other people’s credit cards to purchase publications.	2.85	1.23
12	Manipulation by issuing fake credit cards.	2.98	1.26
13	The stagnation of the university’s internal legal regulations and legislation in light of the huge technological development at the present time.	2.78	1.26
14	The difficulty of applying intellectual property protection in information technology and electronic publications.	2.79	1.20
15	Lack of interest in applying the dimensions of cybersecurity at the university.	2.76	1.16
16	Poor infrastructure and continuous maintenance of software and network systems at the university.	3.15	1.25
17	Poor qualification of the specialized judicial agencies and the judicial police in the field of prosecuting and prosecuting cybercriminals.	3.23	1.12
18	Lack of a clear and binding strategy for those involved in making communication tools and programs and storing and processing information at the university.	3.35	1.12
19	Absence of a professional coding system to preserve the publications of faculty members.	2.93	1.19
20	The reluctance of beneficiaries to purchase original products with intellectual property rights due to their high prices.	3.33	1.06
	Total	3.01	.9601
Ways to overcome cybersecurity practice in Saudi universities			
21	It is essential to use and develop open source tools to achieve the principles of cybersecurity.	4.12	.989
22	It is essential to activate digital identity protection programs based on the electronic signature to ensure the integrity and confidentiality of information.	4.20	.875
23	Data being at the disposal of users.	3.78	1.15
24	It is essential to hire programmers to protect websites for publishing faculty members’ writings.	3.80	1.30
25	It is essential to provide high protection for the privacy of information and maintain its confidentiality.	3.76	1.28
26	It is essential to provide a safe and appropriate electronic environment for marketing the publications of faculty members.	3.18	1.24
27	It is essential to preserve the information, its integrity and consistency	3.02	1.152
28	Ensuring that the physical components of the electronic fund transfer system are not tampered with using the Internet.	2.89	1.194
29	Not allowing unauthorized persons to access the intellectual production of faculty members.	3.12	1.197
30	Protecting university devices and networks from intrusions.	3.02	1.223
	Total	3.49	.711