Awareness and Challenges of adopting Cybersecurity at Health Colleges at Najran University

Shaza Dawood Ahmed Rihan
Computer department , applied college, Najran University, KSA
Corresponding author: Email address: sdrihan@nu.edu.sa

Abstract

Background: In the modern digital age, the issue of cybersecurity has emerged as a highly important issue, affecting various fields around the world including health sector. This research **aimed** to identify the degree of awareness among members of health colleges about cyber-security by demonstrating the extent to which their aware of cyber-security concepts from their point of view, focusing on the experience of Najran University in information security and its evaluation. **Methodology**: Descriptive and analytical approach was used to attain the research objectives, and the case study methodology was used because it is suitable for such types of studies. **Results:** The mean level of Najran University employees' attitude toward the cyber-security concepts was ranked from the most agreement (M=4.00) to the least agreement (M=2.82) among the sample. For the employees' attitude toward the Cyber-security risks was ranked from the most agreement (M=4.06) to the least agreement (M=4.00). While for the mean of level of employees' attitude toward the Cyber-security violations was ranked from the most agreement (M=4.06) to the least agreement (M=4.00). **Conclusion & recommendation:** Our research has revealed the urgent necessity to build a cyber-security plan in order to enhance the cyber ecosystem. Saudi Arabians are more likely to avoid cybercrime since they are aware of the regulations and have a potential balance between Internet usage and awareness. This is critical because cybercrime technology poses a challenge to all of us because it is capable of leaving no trace or evidence. According to our recommendations, future work in this sector should include other elements to match varied educational environments around the world.

Keywords: Cybersecurity, information security, technology, communication networks

Introduction

Notably, higher education institutions, especially health colleges, have become prime targets for cyber-attacks because they possess a wide range of valuable and sensitive information. These colleges store a wealth of personal, financial and research data, making them vulnerable to malicious actors seeking to exploit vulnerabilities in their information systems.

Information technology, High Technology, Information Era, and information Highway, all these terms and others indicate the importance of information[**Cheung, et al., 2011**]. The present-day has become technical and informational. Although, technology and information networks have helped contemporary societies to communicate, on the other hand, they have helped violate the rights and privacy of others[**McDuffie & Piotrowski 2014**]. This led to an increase in security concerns about various infringements on the security and safety of information, and many questions were asked about the systems and policies to protect that information from access and misuse, whether in terms of the scientific technology used or in terms of qualifying human personnel to be able to discover and treat that infringement [**Sedgewick, 2014**]. In line with the new developments and challenges produced by the information and technology revolution, the idea of this study comes to clarify that the protection and security of information is the biggest challenge that the third millennium has raised.

In the world of information technology, cyber security is critical. In our era, protecting information has become one of the most difficult tasks. When we think of cyber security, the first thing that comes to mind is cybercrime, which is on the rise at an alarming rate[**Cheung, et al., 2011& Ghosh, 2019**].

Everything in the third millennium has become dependent on information and communication technology for that information, and its systems have become in constant danger and must be protected from any kind of security threats because its penetration causes many problems at all levels of individuals, institutions, and governments. Therefore, it must be protected by scientific methods and education the employees of Najran University of the need to protect their information[**Sedgewick, 2014**].

Cheung et al discussed how the Challenge-Based Learning (CBL) paradigm can be applied to cybersecurity education. Students generated crucial doubts that represented their interests in information security, crafted difficulties on protecting sensitive data from cyber-attacks, and then devised alternatives to protect their information and network in this research; students competed in two cybersecurity contests against their fellow students from other local universities. Students were required to work together in these realistic real-life challenges, think on their feet, and apply their skills to fight against cyber-attacks. According to their analyses, students' computer and security abilities, enthusiasm in learning security, and ability to teach others improved following the study. They believe that students' learning was enhanced even further when they published their research outcomes and gave presentations to their class fellows[**Cheung, et al., 2011**].

The authors in [**McDuffie & Piotrowski 2014**] present a study on cyber security resilience examination of a shipboard INS installed on a RoPax ship engaged in international trade. The research used a mixed-method technique, which included an interview with the ship's navigational echelons and INS cyber security testing utilizing an industrial vulnerability scanner. The discovered threats were qualitatively evaluated to determine the source of cyber risks posing a threat to the INS. The findings hint at cyber dangers due to flaws in the INS's fundamental operating system, implying that periodic preventative maintenance is needed in addition to compliance issues.

In [**Sedgewick, 2014**], the authors emphasize the need for public-private collaborations in cybersecurity education.

Computer and other related devices used to access information on any of the thing present in the world is covered in the domain typically known as Information technology (IT). Business operations, the company's workforce, and personnel require information technology to access through computers, whether it is storing, retrieving, or manipulating [**Ghosh., 2019**]. Global companies use it to flaunt their products, whereas the local flea market also regularly uses information technology. As information technology has helped millions of people make their everyday lives better, it has somewhat also violated the rights and privacy of others, and this has issued the main reasoning for security. In line with the new developments and challenges produced by the information and technology revolution, the idea of this study came to clarify that the protection and security of information is the biggest challenge that the third millennium has raised **[Thatcher., et al 2018], [Li., et al 2019].**

The rapid development in the Internet and communication and information and their respective technology fields used worldwide have standards for the crime. It all is because of mishandling and misusing the technology, which automatically leads to the rise of new crime issues. These technology-related electronic crimes are carried out through attacks, penetrations, and infiltration within the systems **[Paul & Aithal., 2018**]. A cyber-attack is an "internet attack based on infiltrating unauthorized websites, aiming to disrupt or destroy the available data and then obtain it. It is a set of electronic attacks carried out by a country against another country." Cyber Security plays an important role in the field of information technology. Securing information has become one of the biggest challenges in this era. Whenever we think about cyber security, the first thing that comes to our mind is cybercrimes are increasing immensely day by day. If not handled correctly, sensitive information regarding individuals' identity, financial stockings, and intellectual property can lead to negative consequences. This kind of information must be protected from any security threats as it may cause problems that cannot be tolerated [**Jang-Jaccard & Nepal., 2014], [Mullet., et al 2021**].

Keeping the Internet safer has been one of the biggest strategies nowadays, as electronic crimes are increasing day by day. It has become essential to improve management as a legislative strategy. More secure and extensive practices are needed to maintain and encounter cyber-crimes. Law authorization and police officials need to investigate cyber-crimes efficiently [**Zong., et al 2019]**. Many countries are now compelling strict rules for manifesting cybercrimes and keeping their vital information safe and secure.

In today's world, every individual is facing problems due to cyber security, and over the past 10 years, it has become one of the major concerns in the IT world. Cyber security assault can bring about everything from wholesale fraud to big companies targeted by blackmailing [**Hoffmann., et al 2020],**

[Sivanathan., et al 2017]. As hackers can hack various organizations, enterprises to governmental departments, everyone needs to be aware of these scams and some measures and concerns that can be used to avoid such crimes. Big companies and various organizations get worried about cyber security because, along with losing their confidential data, they can also lose their trusted customers, so everyone in the present world wants to secure their private information without getting hacked [**Hussain., et al 2020**]–[**Alhayani., et al 2021**].

Cybercrimes are drastically increasing day by day because of the emerging technologies; due to these, mankind cannot protect their private information. Internet is growing fast these days. The majority of personal or commercial transactions are processed online **[Rohit., et al 2019**]. Advanced technologies like cloud services, mobiles, e-commerce, internet banking and all these modern tools require an individual's personal information. So, it is important to have an expert who has high excellency in these areas and can maintain a high quality of security and provide a reliable platform to mankind.

Improving and providing necessary security to safeguard sensitive data is now considered the most important priority of countries. Safeguarding the data has now become the top trend all over the world. Different organizations are now taking the lead to keep up with cybercrimes. Different techniques are being applied to cybersecurity [**Tweneboah-Koduah., et al 2018**]. Web servers are one of the first leading stages used for capturing someone's personal information, so one should reliably use a secure program not to fall afterwards. After web servers, mobile networks take up most malicious code preservers, so media deliberation is also at significant risk. A very useful tool that gives people a silver lining when dealing with cyber security is encryption. It's a two-way method which can stop intruders from scrutinizing someone's legal and personal information. It is used to ensure information during travel, and much information is exchanged using different systems networks [**Kumar & Somani 2018**].

Today, half of the population of this world is working or dealing with someone using the Internet, so this area demands prerequisite high-quality security. Cyber security has now become a major issue. To some extent, it has begun to restrict the data in the IT industry and to different fields. Improving cyber security and ensuring that necessary data are vital to each country's security and financial prosperity has become an important feature [**Sleeman., et al 2020**].

Study Methodology

This part of the study was devoted to identifying the methods and procedures that were followed in terms of the type and nature of the study, the study community and its parts, how to develop it and its stability, and what are the statistical methods that used in processing the data to reach the results.

This study was applied in nature and explanatory in terms of purposes, and it was quantitative in terms of mechanism and procedures. The study also adopted the descriptive analytical approach for the purpose of measuring the degree of awareness of the members of the health colleges at Najran University of cyber-security.

This paper firstly determined the level of awareness about the dangers of cybersecurity for affiliates of the Najran University, then detected the rate of Najran University affiliates who had been exposed to security violations; after that, knowing the role of educational institutions in supporting the concept of cyber security and finally inventorying the necessary precautionary measures to avoid risks in Najran University and providing solutions to enhance the concept of cyber security.

The study tool (questionnaire) was built by referring to theoretical literature and previous studies. It was composed of three parts. Part one for studying the employees' attitude toward the cyber security concepts. The second part for assessing the employees' attitude toward the Cyber security risks. And the third part for studying the employees' attitude toward the Cyber Security Violations.

Validity & Reliability

The validity of the tool was verified through two methods, namely content validity and data validity, by presenting the scale after it was prepared to the arbitrators in order to express Their opinions on the validity of the content, the belonging of the phrases and their appropriateness.

Internal consistency validity

Internal consistency is calculated by finding the correlation coefficient between the terms of

each dimension and the dimension to which it belongs.

The results of the statistical analysis of the correlation coefficient, as shown in Tables 1 and 2 indicate that there is a statistically significant correlation at the level of Sig = 0.05 between the scores of each item and the total score of the dimension to which it belongs. This indicates the power of scale in clarifying the direction of the sample towards the questionnaire.

Reliability

The researcher used Cronbach's alpha to calculate the stability of the scale, where its value was 0.787, which indicates high stability, and thus we can be confident of the credibility of the scale in achieving the objectives of the study.

Data management and analysis

After collection, the raw data were checked, cleaned, edited, and analyzed using Software SPSS [version 25]. The frequencies, percentages, means and standard deviations were calculated to describe the profile of the respondents. A one-sample t-test was used to evaluate the difference between the real mean of respondents and the hypothetical mean (=3). A P-value < 0.05 was considered significant Participants answered on the survey using a 5-point Likert-type scale ranges from strongly disagree = 1, disagree = 2, Neutral=3, Agree = 4, and strongly agree = 5. The range from 1 to 5 is classified into three subscales: mean scores range from 1.00 to 1.8 represent very low Agreement; mean scores range from 2.61 to 3.40 represent moderate Agreement; mean scores range from 3.40 to 4.20 represent high Agreement; and mean scores above 4.2 represent very high Agreement.

Results

Research Question 1

What is the Najran University employees' attitude toward the cyber security concepts?

Descriptive statistical analysis of means, standard deviations, and percentages was used to analyze this question.

The mean of the level of Najran University employees' attitude toward the cyber security concepts was ranked from the most agreement (M=4.00) to the least agreement (M=2.82) by sample. As shown in Table 3, the most agreement thing was two items (I am careful not to share my personal information with strangers over the Internet) and (I support educating university employees about cybersecurity concepts)(M = 4.00) indicates a high agreement of this statement, in which 78.8% of the participants either strongly agreed or agreed on this statement. The third thing was (I need training courses in the field of cyber security) (M = 3.94) indicates high agreement of this statement, in which 78.8% of the participants either strongly agreed or agreed with this statement. The final thing was (I use special software to protect my computer from hacking) (M = 2.82) indicates moderate agreement with this statement, in which 63.6% of the participants either strongly agreed or agreed with this statement. The overall mean (M = 3.42) indicates a high agreed-upon dimension.

Research Question 2:

What is the Najran University employees' attitude toward the Cyber security risks?

Descriptive statistical analysis of means, standard deviations, and percentages was used to analyze this question.

The mean of the level of Najran University employees' attitude toward the Cyber security risks was ranked from the most agreement (M=4.06) to the least agreement (M=4.00) by sample. As shown in Table 4, the most agreement thing was item (I avoid bypassing state-imposed laws when using the Internet) (M = 4.06) indicates high agreement with this statement, in which 84.9% of the participants either strongly agreed or agreed on this statement. The second and third thing was (I respect the regulations of the Kingdom of Saudi Arabia in dealing with the Internet) and (I am careful to avoid information that contradicts faith and religion) (M = 3.94), which indicates high agreement with this statement, in which 81.8% of the participants either strongly agreed or agreed on this statement. The overall mean (M = 4.02) indicates a high agreed-upon dimension.

Research Question 3:

What is the Najran University employees' attitude toward the Cyber Security Violations?

Descriptive statistical analysis of means, standard deviations, and percentages was used to analyze this question.

The mean of the level of Najran University employees' attitude toward the Cyber-security Violations was ranked from the most agreement (M=4.06) to the least agreement (M=4.00) by sample. As shown in Table 5, the most agreement thing was two items (I support the university's setting up of a system that prevents access to websites that could harm your device) and (The university's cybersecurity requirements cover vulnerability assessment and remediation) (M = 4.06) indicates high agreement of this statement, in which 84.9% of the participants either strongly agreed or agreed on this statement. The third thing was (I would like to develop cyber security procedures and policies at the university) (M = 4.00) indicates high agreement with this statement, in which 81.8% of the participants either strongly agreed or agreed with this statement. The overall mean (M = 4.04) indicates a high agreed-upon dimension.

Table 1: Pearson correlation coefficient between the terms of each dimension and the dimension to which it belongs

Item	Pearson Correlation	Item	Pearson Correlation	Item	Pearson Correlation
cyber security concepts		**Cyber security risks**		**Cyber Security Violations**	
1	.436*	1	.992**	1	.989**
2	.461**	2	.992**	2	.964**
3	.479**	3	.960**	3	.989**
4	.602**	4	.960**		
5	.433*				
6	.602**				
7	.670**				

Table 2: Pearson correlation coefficient between the terms of each dimension and the Questionnaire

Domain	Pearson Correlation
cyber security concepts	.442*
Cyber security risks	.843**
Cyber Security Violations	.803**

*** Correlation is significant at the 0.01 level.* * *Correlation is significant at the 0.05 level.*

Table 3: Frequencies, Percentage, Means and Standard Deviations of Degree of agreement of Attitudes toward the cyber security concepts

Item	Strongly disagree	disagree	Neutral	agree	Strongly agree	M	(SD)	Rank	P
I always copy my files to an external memory	6.1	21.2	39.4	33.3		3.00	(0.901)	5	1.00
I use special software to protect my computer from hacking	6.1	30.3	39.4	24.2		2.82	(0.882)	7	.245
I keep my personal files in more than one place to avoid theft	6.1	27.3	36.4	30.3		2.91	(0.914)	6	.572
I am careful not to share my personal information with strangers over the Internet		9.1	12.1	48.5	30.3	4.00	(0.901)	1.5	.000
I respect other people's opinions and feelings when discussing a topic in my specialization online		18.2	51.5	18.2	12.1	3.24	(0.902)	4	.133
I support educating university employees about cybersecurity concepts		9.1	12.1	48.5	30.3	4.00	(0.901)	1.5	.000
I need training courses in the field of cyber security		12.1	9.1	51.5	27.3	3.94	(0.933)	3	.000
Total	**2.6**	**18.2**	**28.6**	**36.4**	**14.3**	**3.42**	**(0.477)**		.000

M: Mean, SD: Standard Deviation. P: P-value of a one sample t-test.

Table 4: Frequencies, Percentage, Means and Standard Deviations of Degree of agreement of Attitudes toward the Cyber security risks

Item	Strongly disagree	disagree	Neutral	agree	Strongly agree	M	(SD)	Rank	P
I respect the regulations of the Kingdom of Saudi Arabia in dealing with the Internet		9.1	9.1	54.5	27.3	4.00	(0.866)	2.5	.000
I am careful to avoid information that contradicts faith and religion		9.1	9.1	54.5	27.3	4.00	(0.866)	2.5	.000
I avoid bypassing state-imposed laws when using the Internet		6.1	9.1	57.6	27.3	4.06	(0.788)	1	.000
Total		**8.1**	**9.1**	**55.6**	**27.3**	**4.02**	**(0.825)**		**0.000**

M: Mean, SD: Standard Deviation. P: P-value of a one sample t-test.

Table 5: Frequencies, Percentage, Means and Standard Deviations of Degree of agreement of Attitudes toward the Cyber security risks

Item	Strongly disagree	disagree	Neutral	agree	Strongly agree	M	(SD)	Rank	
I support the university's setting up of a system that prevents access to websites that could harm your device.		6.1	9.1	57.6	27.3	4.06	(0.788)	1.5	.000
I would like to develop cyber security procedures and policies at the university.		9.1	9.1	54.5	27.3	4.00	(0.866)	3	.000
The university's cybersecurity requirements cover vulnerability assessment and remediation.		6.1	9.1	57.6	27.3	4.06	(0.788)	1.5	.000
Total		7.1	9.1	56.6	27.3	4.04	(0.798)		**0.000**

M: Mean, SD: Standard Deviation. P: P-value of a one sample t-test.

Discussion

The need for cyber-security in health colleges is multifaceted and increasingly important in today's digital age. As these colleges continue to integrate technology into their educational process they become more attractive to cyber-attacks, making strong cyber-security measures essential.

First, health schools handle a vast amount of sensitive data, including personal information of students and staff, financial records, and intellectual property.

This data is vulnerable to cyber-attacks. Second, the academic environment often encourages open access to information and collaboration, which, while beneficial for research and learning, can create vulnerabilities in IT systems. This open access culture requires a balance between accessibility and security to ensure that research and education activities can continue without compromising critical data. In addition, with the increasing reliance on digital platforms for distance learning and electronic systems used in administration, any disruption caused by cyber-attacks can severely impact those operations.

For example, a ransomware attack can prevent administrators from accessing systems, delaying academic operations and causing significant inconvenience to students and faculty. Tuwhidi and Pridmore reported that Cyber-security skills in information systems are also in high demand, highlighting the importance of preparing graduates who can address these challenges[**Towhidi, & Pridmore 2023**]. This demand underscores the need for higher education institutions to integrate cyber-security into their curricula, equipping students with the skills to protect against cyber-threats.

A recent study by Ferrari and AKhmelevsky used the NICE framework to highlight the importance of understanding, skills, and abilities to meet cyber-security needs. The framework serves as a valuable tool that effectively aligns cyber-security education with industry requirements. To fill industry gaps, the

National Institute of Standards and Technology advises educational institutions to align their programs with the NICE framework [**Ferrari and AKhmelevsky 2024**].

Cyber-attacks are becoming more prevalent across all sectors, especially those targeting health colleges. This has sparked increased interest in cyber-security measures. To protect the personal and sensitive information of students and staff, higher education networks must implement a sophisticated set of accessible platforms and strong security measures. Unfortunately, Attackers have identified educational institutions as prime targets for data theft, as these institutions store vast amounts of valuable information. Additionally, many colleges have adopted a more transparent approach, allowing quick and efficient access to their websites for students. For instance, King Faisal University[**Koshiry., et al 2023**]. There is no doubt that a weak security system policy has a significant impact on cyber-security.

To improve cyber-security, administrators should consider implementing firewalls in educational institutions. Firewalls can indirectly prevent some cyber threats.

In addition, within large university organizations, the presence of untrained staff can lead to direct access attacks. This can exacerbate cyber threats. Therefore, it is the responsibility of the institution to implement training and awareness programs aimed at increasing the awareness of computer users. The presence of such programs indirectly instills a sense of responsibility among employees to protect user data. Employees will put more effort into gaining proper knowledge of using the system and prioritizing safety measures. Finally, lack of support from senior management contributes to the weakness of cyber systems. If senior authorities refuse to allocate additional funds to strengthen the system, higher education institutions will face many challenges. Managers must realize their responsibility to strengthen their institutions' security systems to prevent information leakage. Therefore, they should invest in modern research laboratories and focus more on individual and group research and development in the field of cyber security. This is a necessary measure. In order to increase the security levels in health colleges, it is necessary to establish a strong security system. Research in information systems education highlights the need to shape information systems courses in line with the current requirements of universities.

Conclusion

According to current trends, cybercrime will have an unclear future because the criminals will always be one step forward for the law enforcement agencies. Cybercriminals are always inventing new ways to perpetrate crimes. If authorities want to catch up with cybercriminals, they must improve their skill levels. Cybercriminals always seem to come up with new ways to deceive people. Cybercrime is on the rise, and there is a strong probability it will continue to rise. Traditional laws and technical measures are no longer sufficient in the light of computer crimes.

Modern computer-assisted and Internet crimes have been on the rise as technology has advanced, and more research into the current state of cybercrime and computer forensics in the Middle East, notably Saudi Arabia, is needed. In this paper, we explored general concepts about cyber security and awareness of the dangers and challenges that information is exposed to, focusing on the health colleges in Najran University's experience in information security.

Eventually, this study suggested factors for reducing cybercrime and increasing security awareness among the employees . As a result, these elements will assist administration and decision-makers in formulating plans that will substantially impact anti-cybercrime. In other words, our research has revealed the urgent necessity to build a cyber-security plan to enhance the cyber ecosystem. This research is designed to raise awareness among employees., thereby assisting in the battle against internet abuse.

References

R. S. Cheung, J. P. Cohen, H. Z. Lo, and F. Elia, "Challenge based learning in cybersecurity education," in Proceedings of the International Conference on Security and Management (SAM), 2011, p. 1.

E. L. McDuffie and V. P. Piotrowski, "The future of cybersecurity education," Computer (Long. Beach. Calif)., 2014; 47(8):pp. 67–69.

A. Sedgewick, "Framework for improving critical infrastructure cybersecurity, version 1.0," 2014.

J. Ghosh, "The blockchain: opportunities for research in information systems and information technology," J. Glob. Inf. Technol. Manag.,2019; 22(4):235–242.

J. B. Thatcher, R. T. Wright, H. Sun, T. J. Zagenczyk, and R. Klein, "Mindfulness in information technology use: Definitions, distinctions, and a new measure," MIS Q.,2018; 42(3):pp. 831–848.

L. Li, W. He, L. Xu, I. Ash, M. Anwar, and X. Yuan, "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior," Int. J. Inf. Manage.,2019; vol. 45, pp. 13–24.

P. Paul and P. S. Aithal, "Cyber crime: challenges, issues, recommendation and suggestion in Indian context," Int. J. Adv. Trends Eng. Technol.,2018; 3(1):pp. 59–62.

J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," J. Comput. Syst. Sci., vol. 80, no. 5, pp. 973–993, 2014.

V. Mullet, P. Sondi, and E. Ramat, "A review of cybersecurity guidelines for manufacturing factories in industry 4.0," IEEE Access,2021; vol. 9, pp. 23235–23263.

S. Zong, A. Ritter, G. Mueller, and E. Wright, "Analyzing the perceived severity of cybersecurity threats reported on social media," arXiv Prepr. 2019; arXiv1902.10680.

R. Hoffmann, J. Napiórkowski, T. Protasowicki, and J. Stanik, "Risk based approach in scope of cybersecurity threats and requirements," Procedia Manuf.,2020; vol. 44, pp. 655–662.

A. Sivanathan, F. Loi, H. H. Gharakheili, and V. Sivaraman, "Experimental evaluation of cybersecurity threats to the smart-home," in 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2017; pp. 1–6.

A. Hussain, A. Mohamed, and S. Razali, "A review on cybersecurity: Challenges & emerging threats," in Proceedings of the 3rd International Conference on Networking, Information Systems & Security, 2020; pp. 1–7.

Y. K. Dwivedi, G. Kelly, M. Janssen, N. P. Rana, E. L. Slade, and M. Clement, "Social media: The good, the bad, and the ugly," Inf. Syst. Front.,2018; 20(3):pp. 419–423.

Z. Zhang and B. B. Gupta, "Social media security and trustworthiness: overview and new direction," Futur. Gener. Comput. Syst.,2018; vol. 86, pp. 914–925.

B. Alhayani, H. J. Mohammed, I. Z. Chaloob, and J. S. Ahmed, "Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry," Mater. Today Proc., 2021.

K. Rohit, V. A. Babu, and K. R. Reddy, "Cyber Security," HOLISTICA–Journal Bus. Public Adm.,2019; 10(2): pp. 115–128.

S. Tweneboah-Koduah, A. K. Tsetse, J. Azasoo, and B. Endicott-Popovsky, "Evaluation of cybersecurity threats on smart metering system," in Information technology-new generations, Springer, 2018, pp. 199–207.

S. Kumar and V. Somani, "Social media security risks, cyber threats and risks prevention and mitigation techniques," Int. J. Adv. Res. Comput. Sci. Manag.,2018; 4(4): pp. 125–129.

J. Sleeman, T. Finin, and M. Halem, "Temporal Understanding of Cybersecurity Threats," in 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), 2020; pp. 115–121.

Towhidi, G. and Pridmore, J. "Aligning Cybersecurity in Higher Education with Industry Needs." In: Journal of Information Systems Education, (2023); 34(1): pp. 70-83.

Ferrari EWong and AKhmelevsky Y: Cybersecurity Education within a Computing Science Program - A Literature ReviewProceedings of the 26th Western Canadian Conference on Computing Education. 2024; 10.1145/3660650.36606661-5Online publication date: 2-May-2024. https://dl.acm.org/doi/10.1145/3660650.3660666

Amr El Koshiry, Entesar Eliwa, Tarek Abd El-Hafeez, Mahmoud Y. Shams: Unlocking the power of blockchain in education: An overview of innovations and outcomes. J. of Blockchain Research and Applications, 2023; 4(4): 100165