Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P) Vol.11 No.2, 2022, pp.20-24
© The Research Publication, www.trp.org.in
DOI: https://doi.org/10.51983/ajcst-2022.11.2.3448

Importance of Cyber Security in the Higher Education Sector 2022

Kamal Aldin Yousif Yaseen
Department of Information System, CEMIS College, University of Nizwa, Nizwa, Oman
E-mail: k.yousif@unizwa.edu.om

(Received 16 August 2022; Accepted 5 October 2022; Available online 15 October 2022)

Abstract - **Today, we are witnessing the widespread of the digital revolution and its applications in all fields, as the means of networking provided the exchange of information, experiences, and knowledge in all sectors, but with all these positive features, we find that today's digital world has brought a wide range of risks of its own, such as attacks and malicious programs like viruses, worms, spyware files, etc. and the education sector higher education is not far from these negative influences that hinder the education process and affect its infrastructure and its periphery, including students, teachers, administrative assistants, the environment and teaching methods. For this risk, we need to awareness and cyber security training and adopt a solid cyber security policy in higher education sectors institution in order to protect this vital sector. This research paper will explore the importance of cybersecurity in this sector and provide the strategies that students, faculty, and staff can utilize to promote cybersecurity across higher education institutions.**

Keywords: **Education, Cyber Security, Threats, Platforms, E-Learning, Policies**

I. INTRODUCTION

We live these days in light of the massive spread of the digital information revolution, which has made the world a better place and facilitated the means of communication to the far end, with its many systems, applications, and technologies. Ransomware, fraud, identity theft, and the higher education sector are not far from these risks, it has been observed as very high in the list of targets of cybersecurity attacks as most studies have shown that various educational institutions are exposed to 30% of denial-of-service attacks and ransomware attacks that negatively affect the reputation of these institutions and the workflow in them. Therefore, this study examines how to protect assets, students, teachers, and preservation on the integrity of data in higher education institutions because of its great importance and the provision of strategies, standards, advice, and guidance necessary to implement the task of protecting these institutions from surrounding and potential risks.

A. Cyber Security

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources including hardware, software, firmware, information/data, and tele-communications, in our lived reality, we find that most educational institutions ignore the importance of cybersecurity, which casts a negative shadow on the data and the entire educational process. Below we take a look at the data that is available in these institutions:

B. Financial Data

These institutions collect, store and process a set of financial data that includes bank account information for employees and students, as well as the accounting and financial cycle of internal procedures. This important information could be misused by third parties or others.

C. Personally Identifiable Information (PII)

Students and employees are prime targets for identity and information theft attacks, cross-site programming attacks, spying attacks, etc.

D. Enterprise Data

Information of students, faculty, and administrative staff from registration procedures, tuition fees, courses, scientific research, student results, and their quarterly reports may be targets internally or external attack aimed at either modifying or not making it available, and certainly it must be protected because tampering with it jeopardizes the reputation, competitiveness, and fairness of institutions [2].

E. Educational Data

Scientific research and evaluation methods are among the matters and other vital educational activities and tasks for educational institutions and exposing them to exposure exposes these institutions to a number of procedures and possibly penalties [3].

II. CYBER SECURITY THREATS

Cyber Security threats are defined as any digital activity that could threaten the integrity of content or endanger access to data and the privacy of users. Here is a list of common threats.

A. Cyber Terrorism

This threat is a politically based attack on computers and information technology to cause harm and create widespread social disruption.

B. Malware

It’s Software that enters a computer system without the owner’s knowledge or consent, malware is any software intentionally designed to cause damage to a computer, server, client, or computer network, the three primary objectives of malware is to infect a computer system Conceal the malware’s malicious actions bring profit from the actions that it performs.

C. Trojans

These threats also aim to create a backdoor on your computer that gives malicious users access to your system, possibly allowing confidential or personal information to be compromised. Unlike viruses and worms, trojans do not reproduce by infecting other files nor do they self-replicate.

D. Botnets

It’s hundreds or thousands of zombie computers are under the control of an attacker Zombie An infected computer with a program that will allow the attacker to remotely control it.

E. Adware

This threat delivers advertising content, often as pop-up windows that can slow or crash a computer can monitor or track the user’s activities.

F. SQL Injection

Attackers insert SQL malicious code inside the website in order to request or change the database contents.

G. Phishing

Phishing is described as a fraudulent activity that is done to steal confidential user information such as credit card numbers, login credentials, and passwords.

It is usually done by using email or other forms of electronic communication by pretending to be from a reliable business entity.

H. Man in the Middle Attack (MITM)

This status occurs when the attacker is located among the communication channels and monitoring the contents which are sent or received across the channels; it may interrupt or change the data nature or destinations.

I. Denial of Service (DoS)

It is a service availability attack by flooding the network with a large number of messages until the server stops responding to user requests.

J. Viruses

It’s malicious code Programs that secretly attach to a file and execute when that file is opened, once a virus infects a computer, it performs two separate tasks.

In addition to these common threats which was mentioned before also the higher education institutions suffer from a number of bad cultures and practices as the following:

1. Decentralized IT

Most departments and colleges in higher education institutions adopt different and diverse networks and systems that meet their needs, which makes imposing a single security policy difficult.

2. BYOD Culture

Most institutions encourage students and employees to use their own devices and thus store their lessons and work and manage what their parents abide by cybersecurity standards or download the necessary protection programs here tight security policy must be clarified in this regard.

3. Open Networks

Much higher education institutions use open networks to allow freedom of information between their peers, staff, or faculty and they do not clarify the policies of entry and use of a court, and therefore attackers and other threats can exploit these fatal gaps and enter the system due to the lack of control and protection

4. Internal Threats

According to many studies, internal attacks are more common than external ones because most organizations focus on ways to protect against external attacks and neglect internal ones, which enable the use of e-mail or portal contents to attack enterprise resources, in addition to unintended human errors that can cause adata breach.

III. OBJECTIVES OF THE STUDY

Previously, many serious scientific pieces of research were conducted regarding the importance of cybersecurity in the education sector, especially higher education, but only a few of them focused on the policies and standards that must be applied so that these institutions can overcome the danger of many threats and risks.

Hence, this study focuses on policies, standards, and measures. And the instructions to be followed in the various institutions of higher education. In this study, the risks and challenges were discussed, as well as the importance of imposing policies and standards to meet the escalating cybersecurity challenges in higher education institutions.

IV. METHODOLOGY

This paper examines the importance of cybersecurity in the higher education sector by clarifying the various risks that can affect the educational environment in this important sector, such as attacks, viruses, Trojan horses, denial-of-service attacks, and others, accompanied by the importance of guidance, advice, security standards and policies that can reduce or prevent risks. This research also sheds light on the research studies conducted in cybersecurity regarding the education sector and includes multiple databases in the period from 2018 to 2022.

V. DISCUSSION

To discuss this study, and with the love of the latest statistics, the education sector has ranked sixth most targeted by attacks, as it ranked second for ransomware attacks, and thus has been classified as the least secure among other sectors, with a rate of more than 30% of exploitable security vulnerabilities, affecting about 12% of employees and students. Most of the attacks that the education sector suffers from are social engineering attacks, which amounted to 41%, and we find that a percentage of universities agree more funding must be provided for IT security to protect the intellectual property of important research. We also find that 87% of educational institutions have experienced at least one successful attack in the last decade. Including higher education institutions [4], [5].

The cyber security market is expected to grow due to the increase and diversity of attacks and security risks, which negatively affected data breaches, the spread of electronic crimes, the entry of so-called digital terrorism, digital warfare, and attacks that do not depend on any users or victims' action (Zero_Click_Attack) and cause great damage. Expect growth from $217 billion in 2021 to $345 billion by 2026, posting a Compound Annual Growth Rate (CAGR) of 9.7% from 2021 to 2026 [6].

The education sector accounted for 13% of all data security breaches during the last few years, sixty percent of data breaches are caused by vulnerabilities that might have been averted if a security update or patch had been deployed. Hence the next graphs show the importance and impact of cyber security on the education sector and cover the most important threats and challenges. This study shows that 40% of attacks in the higher education sector are due to social engineering attacks, 30% are because of failure to address fishing attack issues, and 17% of education institutions pay ransom to restore their data [7].

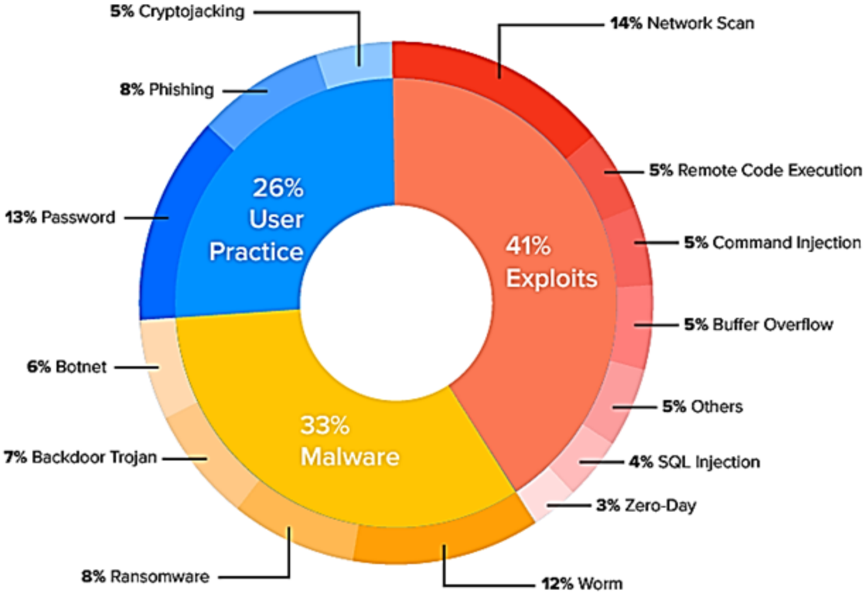

Fig. 1 Cyber security threats

Fig. 1 and 2 shown that different malware could lead to 41% of exploits and the attackers can gain access by using those threats to the system and making huge damage, also the lack of awareness and adopting unappropriated security policies and bad user behaviour's lead to 26% of threats as well as the graph shown that the malware is still the big challenge to the cyber security and the education institutions should following all necessary efforts and enforcing the security policies in order to protect them self from threats [8], [19].

Fig. 3 shows the percentage of organizations over time where cyber security is seen as a high priority for directors, trustees, and other senior managers.

Fig. 4 shows the suffering of the education sector's greatest share of cyberattacks among the other sectors and that gives the departments of information technology and cyber security the responsibility to plan and adopting solid cyber security policies to secure the networks and systems [10], [11].

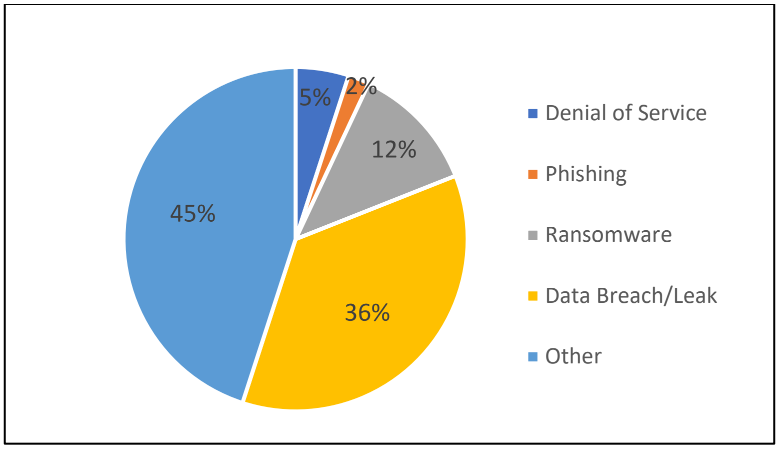

Fig. 2 Cyber-attacks in the education sector

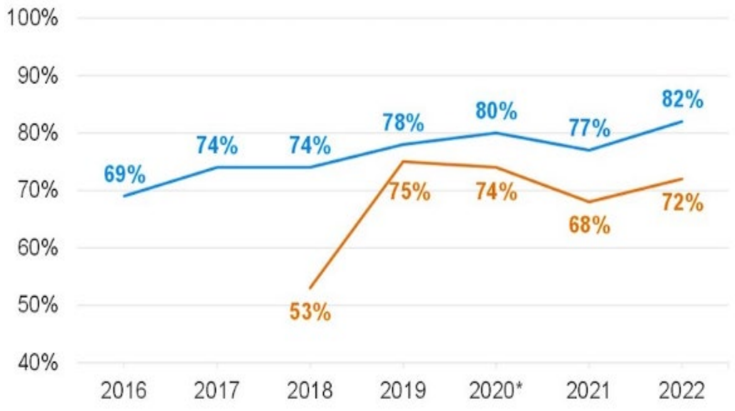

Fig. 3 Percentage of Cyber Security Impact

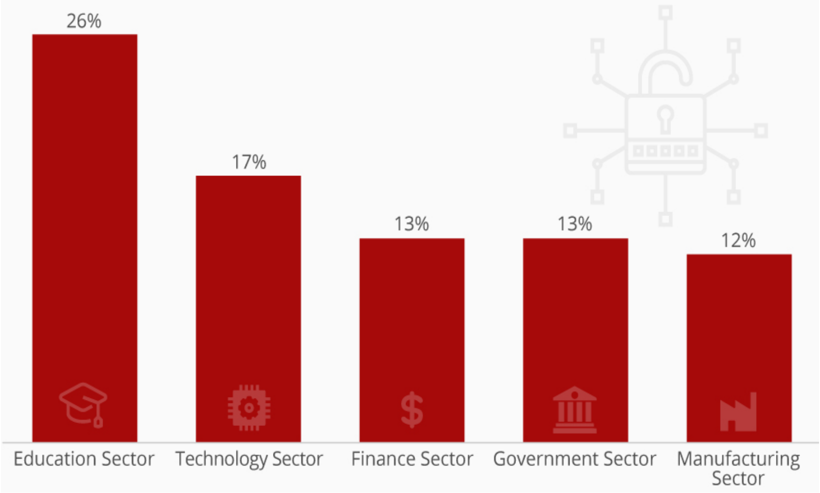

Fig. 4 Suffering of Education Sector from Cyber Attacks

VI. RECOMMENDATIONS

Academic institutions must take appropriate precautions for students' security despite limited resources. Some effective measures are

1. Implement a solid cyber Security policy, to prevent all the education sector environment.
2. Installing the threats preventers tools and devices such as firewalls, IDS, NIDS AND IPS in order to overcome and mitigate the risk.
3. Adopt strong access policies to prevent unauthorized access to the network and limit the use of personal computers by staff, students and faculty to complete work tasks.
4. Continuous awareness of the dangers of security threats by conducting workshops and courses for associates.

5. Training IT staff to understand the nature of attacks, risks, and how they occur, with an emphasis on how to exploit vulnerabilities, preventive measures, and work protocols. Identify the most valuable IT assets and secure them by using a robust security solution.

VII. RESULTS OF THE STUDY

1. Educational institutions are very important and vital, and therefore they must be protected from attacks and risks to ensure their continuity to perform their great roles.
2. This study proved that educational institutions are still exposed to many security risks and attacks targeting data and information dumping, competitiveness and intellectual property issues, and targeting students.
3. Security policies can reduce all these risks and increase the productivity of students, faculty, and administrative staff.
4. The education sector itself can contribute to eliminating cyber-attacks by adopting, sponsoring, and establishing relevant disciplines, and spreading the culture of precautions, risk reduction, and awareness.
5. Most of the threats can be overcome with a few measures, awareness, and correct and inexpensive practices.

VIII. CONCLUSION

The importance of cyber Security in the higher education sector considering all the development that witnessing in light of the increasing attacks and risks makes it necessary to follow all measures and tools necessary to curb these threats so as not to affect the education environment and weaken its outputs. For important tips and instructions for protection, with a focus on studying risks and ways to protect them and researching a group of previous studies in cybersecurity. However, a lot of these businesses are open to online attacks and educational institutions should follow security policies in order to protect their valuable assets. Also, this paper examined the various risks and how to deal positively with them [12], [13], [14], [15].

REFERENCES

[1] F. Khalid, “Understanding university students’ use of Face book for collaborative learning,” *International Journal of Information and Education Technology*, Vol. 7, No. 8, pp. 595-600, August 2020.

[2] F. Annasingh and T. Veli, “An investigation into risks awareness and e-safety needs of children on the internet,” *Interactive Technology and Smart Education,* Vol. 13, No. 2, pp. 147-165, 2019.

[3] L. Muniandy and B. Muniandy, “The impact of social media in social and political aspects in Malaysia: An overview,” *International Journal of Humanities and Social Science,* Vol. 3, No. 11, pp. 71-76, 2013.

[4] V. Ratten, “A cross-cultural comparison of online behavioral advertising knowledge, online privacy concerns and social networking using the technology acceptance model and social cognitive theory,” *Journal of Science & Technology Policy Management,* Vol. 6, No. 1, pp. 25-36, 2015.

[5] M. D. Griffiths and D. Kuss, “Online addictions, gambling, video gaming, and social networking,” *The Handbook of the Psychology of Communication Technology*, Chichester: John Wiley, pp. 384-406, 2015.

[6] L. Mosalanejas, A. Dehghani and K. Abdelhadi, “The students’ experiences of ethics inonline systems: A phenomenological study,” *Turkish Online Journal of Distance Education,* Vol. 15, No. 4, pp. 205-216, 2014.

[7] D. Kotido, N. Teokleous and A. Zahariadou, “Exploring parents’ and children’s awareness on internet threats in relation to internet safety,” *Campus-Wide Information Systems,* Vol. 29, No. 3, pp. 133-143, 2012.

[8] N. Ahmad, U. A. Mokhtar, Z. Hood, *et al.,* “Cyber security situational awareness among parents,” presented at the *Cyber Resilience Conference, Putrajaya Malaysia*, pp. 7, 13-15 November 2019.

[9] R. S. Hamid, Z. Yunos, and M. Ahmad, “Cyber parenting module development for parents,” *in Proc. INTED2018 Conference*, Valencia, Spain, 5th-7th March 2018.

[10] F. Khalid *et al.,* “An investigation of university students’ awareness of cyber security,” *International Journal of Engineering & Technology,* Vol. 7, pp. 11-14, 2018.

[11] C. S. Kruse *et al.,* “Cyber security in healthcare: A systematic review of modern threats and trends,” *Technology and Health Care,* Vol. 25, No. 1, pp. 1-10, 2017.

[12] P. Dong *et al.,* “A systematic review of studies on cyber-physical system security,” *International Journal of Security and Its Applications,* Vol. 9, No. 1, pp. 155-164, 2015.

[13] U. Franke and J. Brynildsen, “Cyber situational awareness, A systematic review of the literature,” *Computers & Security,* Vol. 46, pp. 18-31, 2014.

[14] N. H. A. Rahim *et al.,* “A systematic review of approaches to assessing cyber security awareness,” *Kubernetes*, 2015.

[15] D. Mellado *et al.,* “A systematic review of security requirements engineering,” *Computer Standards & Interfaces,* Vol. 32, No. 4, pp. 153-165, 2010.