IJCSEInternational Journal of Computer Sciences and Engineering Open Access
Review Paper Vol. 9, Issue.12, December 2021 E-ISSN: 2347-2693

Review on Major Cyber security Issues in Educational Sector

Ankita sharma

Assistant Professor CSE, Chandigarh University Punjab, India

Author's Mail Id: ankita.ceh@gmail.com

DOI: https://doi.org/10.26438/ijcse/v9i12.2629 | Available online at: www.ijcseonline.org

Received: 02/Dec/2021, Accepted: 04/Dec/2021, Published: 31/Dec/2021

***Abstract*-** The demand for information security in higher education will continue to grow. A lack of risk management has already resulted in catastrophic data breaches, and these incidents are expected to continue. Academics, students, and universities around the world have been subjected to a constant torrent of attacks. This study relies on a review of several educational surveys. As a result of this research, new lines of study will be opened up for higher education security. Various sources have been analysed in this report to provide an overview of cyber security challenges. We categorise our review mostly based on the research questions that we address. In order to gain a foothold in the educational community, it will be beneficial to both corporations and academics.

***Keyword*-** Threats, Virtual learning Environment, Issues, E-Learning

I. INTRODUCTION

Universities and academic institutions have become profitable targets for cyber-attacks, with many high-profile events already occurring.[1]According to a new analysis, the education sector in India was targeted substantially more than other industries in the month of July, with an average of 5,196 attacks per week**[2].** Academic institutions are appealing targets for cyber-criminals, espionage, and hacktivists because they manage enormous volumes of valuable research and sensitive personal data.[3]. There are a number of cultural concerns to address, including combining security measures with academic openness and free flow of knowledge, which institutions are attempting to promote [4] Collaboration and information sharing with other researchers, both inside and outside the university, is a security challenge that may be unheard of in other businesses. Universities' interconnection continues to develop, and the attack surface grows in lockstep. Organized criminal groups like as The Silent Librarian Campaign [5] are challenging the traditional openness and sharing ethos in academia, where cyber security worries are now migrating to the board room. Thousands of publications have been published in academic journals about cyber security, yet the higher education sector frequently defers to technicians to resolve the problem.

Only with rise of technology, knowledge, which gave our period its name, has become much more prevalent in all aspects of life. Irrespective of the industry, institutions that have and use information in a timely and efficient manner get a competitive edge and achieve their objectives faster. Information, because of its importance, necessitates the establishment of required safeguards for its security. The idea of data protection has been introduced into our everyday to secure information from inadequately institutions or individuals who may pose a harm to it.

Infosec risk can be defined by best practices in terms of assets, threats, vulnerabilities, and events [6,7]. Nevertheless, because information systems are constantly created, processed, and stored, recognizing them within an organization can be difficult. Second, the threat landscape in ict is always evolving, making it difficult to recognize, evaluate, and map detrimental threats to an organization due to new tactics and tools. Finally, organization design changes can reveal previously unknown vulnerabilities Universities and higher educational (HE) institutions often engage training, growth, and researching that has a significant societal impact. Both the public and private sectors. As a result, the goal of this essay is to review the available literature and synthesize cyber security expertise, vulnerabilities, and research HE security trends. The methodology of paper focus on the following HE-related questions (RQ) , shown in Figure 1 :

1. In HE, what are the most common threats and events?
2. What are the most common risks ?
3. What are the detection techniques to solve Cyber security in HE?

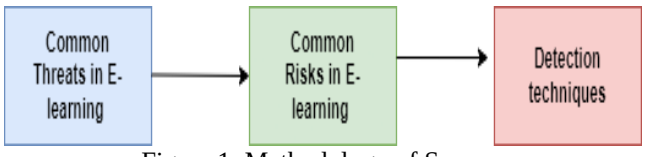

Figure 1: Methodology of Survey

The systematic literature review method is used to resolve these issues. The risks of breaking rules and regulations are not addressed in this study because they vary by location and country. The systematic literature review method is used to resolve these issues. The risks of

breaking rules and regulations are not addressed in this study because they vary by location and country. The study is intended for both academics who are investigating cybersecurity and professionals who are actively involved in HEI cybersecurity.

This paper structure in following , Section 2 present the literature review which help reader to understand the background , knowledge .Section 3 , provide the results of the research questions from the different literature . Section 4 will conclude the the work .

II. RELATED WORK

Some research publications on information security at HE were found in our literature review, but they were not relevant for our Comprehensive Literature Review (CLR). There were no prior studies of cybersecurity concerns in higher education that we could find.The closest thing we discovered was Bongiovanni's [1] literature evaluation of information security management in HE, which included literature on control systems and other related topics. Cyber behaviors, standards, information security regulations, social and technical alternative therapies, technical solutions and Administration, as well as culture and awareness Another piece written by him is a review article by Chen.The reader will find samples of similar papers in this section. Adams and Blanford [8] investigated security in online courses in 2003 and discussed the security-availability trade-off. The writers were maybe the first to have a complete overview of (North American) academia's security culture and issues with standard security departments. Whitman and Mattord in 2016 [9] mapped cybersecurity threat agents, events, and risks for generic industry, which served as a motivation for our research.

Beaudin [10,11] explores the legal ramifications of data breaches in higher education while keeping student data, as well as state and federal cybersecurity regulations. Hussain et al. [12] look at the risks of online social networking in Malaysian higher education, concentrating on the cybersecurity risk to professors. A related study [13] concentrates on the cybersecurity vulnerabilities that university libraries face.

Numerous spoofing and social engineering studies of students and staff in higher education have been undertaken, for example, Diaz et al. [14] and Cuchta et al. [15], both of which indicate a high level of sensitivity to phishing attempts in academia. Dadkhah [16], in relation to phishing assaults, examines cyber-attacks in scholarly publishing, such as the fraudulent call for papers, and the attackers' techniques for deceiving researchers.

Teixeira da Silva [17] also looked at the problems and costs of spam emails in academia. A underlying cause assessment of physical security concerns at a University College was undertaken by Wangen et al. [18]. Kashiwazaki [19] describes a data breach incident that occurred at a Japanese university. Table 1, describe the comparative analysis of the literature survey.

Table 1. Comparative Analysis Of the literature Survey

Sr No.	Paper	Description	Gap
1.	How Safe Is Your Data? Cyber-Security in Higher Education. HEPI Policy [8]	Investigated security in online courses in 2003 and discussed the security-availability trade-off.	The writers were maybe the first to have a complete overview of (North American) academia's security culture and issues with standard security departments
2.	Threats to Information Protection-Industry and Academic Perspectives: An annotated bibliography[9]	The mapped cyber security threat agents, events, and risks for generic industry, which served as a motivation for our research	-
3.	The Legal Implications of Storing Student Data: Preparing for and Responding to Data Breaches. New Dir. Institutional[10]	Explores the legal ramifications of data breaches in higher education while keeping student data, as well as state and federal cyber security regulations.	Data breaches in higher education
4.	The least secure places in the universe? A systematic literature review on information security management in higher education[11]	The literature evaluation of information security management in HE, which included literature on control systems and other related topics	Cyber behaviors, standards, information security regulations, social and technical alternative therapies, technical solutions and Administration, as well as culture and awareness
5.	Risk and Threat via Online Social Network among Academia atHigher Education[12]	The look at the risks of online social networking in Malaysian higher education, concentrating on the cyber security risk to professors	
6.	Review of Trends and Issues of Cybersecurity in Academic[13]	The concentrates on the cybersecurity vulnerabilities that university libraries	spoofing and social engineering studies of students and staff in

		face.	higher education have been undertaken
7.	in an Academic Community: A Study of User Susceptibility and Behavior[14]	The both of which indicate a high level of sensitivity to phishing attempts in academia	
8.	Factors in Cybersecurity[16]	The relation to phishing assaults, examines cyber-attacks in scholarly publishing, such as the fraudulent call for papers.	The attackers' techniques for deceiving researchers.
9.	An empirical study of root-cause analysis in information security management.[19]	also looked at the problems and costs of spam emails in academia.	Problems in email server

III. RESULTS

Acts undertaken by malicious attackers to obtain access to assets are known as threat occurrences or attacks. To acquire access to systems in higher education, these agents could use a variety of assault tactics. The parts that follow will give literary sources that demonstrate a rundown of the most prevalent HEI-related attacks and threats Let's begin with articles. Before summarizing, focus on SOC statistics and publishing data breaches the outcomesThe researchers focus is addressed in this study. HE-related questions (RQ):

3.1. In HE, what are the most common threats and events?

The most common threat is data breaching in the system of the higher education institutions.

I. Payment Card Fraud(CARD) : Fraud involving debit and credit cards that is not carried out through the use of a hacking tool
II. Unintended disclosure : Sensitive data in the website which publicly available.
III. Hacking and malware : Electronic entry by outside party or data loss by spyware and malware .
IV. Stationary devices: Lost the data , stolen stationary electronic devices.

3. 2. What are the most common risks ?

Methods such as virtual private networks (VPNs), proxy servers, and infiltrated systems all aid the threat agent in concealing his genuine identity, making attribution notoriously difficult [68]. The internet is used by billions of individuals, and a threat agent can be anything from a state-sponsored entity looking to steal information to a curious "script kiddie."

1. Data loss : Data loss that is unrecoverable is a terrifying possibility. Ransomware encrypts data and demands payment in exchange for its decryption. Ransomware can infiltrate a network through a variety of methods, including phishing emails, software flaws, BYOD, and other cyber attempts.
2. Financial Fraud : The data show that cyber-crime is the most serious threat to academic institutions. This actor, mostly driven by financial gain, infests systems and procedures in search of financial and transaction data to exploit.
3. Loss of service Availability : When it comes to services like internet access, email systems, and digital libraries, universities are high-availability enterprises. If vital services are unavailable, most universities' core processes will suffer quickly.

3.3 What are the detection techniques to solve Cyber security in HE?

Universities are high-availability organizations when it comes to services like internet access, email systems, and digital libraries. Most universities' key procedures will suffer fast if vital services are missing.

1. Machine learning techniques[19] : Machine learning (ML) is the study of computer algorithms that can learn and develop on their own with experience and data.
2. Deep neural Network : An ANN having numerous hidden layers between the input and output layers is known as a deep neural network (DNN). DNNs can represent complex non-linear relationships in the same way as shallow ANNs can.
3. Security Algorithm[20] : The term "security algorithm" refers to a mathematical process for encrypting data. Information is encoded, and it takes a software key to decode it and restore it to its original state. Our Security Algorithms Experts Group

IV. CONCLUSION

Despite the fact that the number of research publications on cybersecurity is rapidly increasing, our findings reveal that empirical research on security practises in higher education is woefully deficient. The question arises as to whether he wants to entrust this vital task to commercial security providers. Despite being assembled from sources of various repute, the sources mainly agreed on the following for HE: PII on students and employees, financial data, research data, IP, student grades, and administration details are the most valuable assets managed in academia. Intrusion, malware, and other forms of compromise were the most common threats. This help researcher to understand the need of work in this field.

ACKNOWLDEGMENT

A sincere vote of gratitude to Department of Computer Science and Engineering oF Chandigarh university for give a knowledge about the concepts of security and platform for enhancing my knowledge in the domain security.

REFRENCES

[1] Bongiovanni, I. The least secure places in the universe? A systematic literature review on information security management in higher education. Comput. Secur. **86, 350–357, 2019.**

[2]Report on Business-standard. Available on: https://www.business-standard.com/article/technology/indian-tops-global-cyber-attacks-on-education-sector-report-121081801000_1.html

[3] FireEye, Inc. Cyber tHreats to the Education Industry. White Paper, 2016. Library Catalog. Available online: www.fireeye.com (accessed on **28 January 2021**).

[4] Adams A; Blanford," A. Security and Online Learning: To Protect and Prohibit. In Usability Evaluation Of Online Learning Programs"; IGI Global: Hershey, PA, USA, **pp. 331–359, 2003.**

[5] J. ChapmanHow Safe Is Your Data? Cyber-Security in Higher Education. HEPI Policy Note, April ISO/IEC 27002:2013 Information Technology–Security Techniques–Information Security Risk Management; Standard; InternationalOrganization for Standardization: Geneva, Switzerland, **2018.**

[6] G.Wangen,C.Hallstensen ,E.Snekkenes "A framework for estimating information security risk assessment method completeness.Int. J. Inf. Secur. **2017**.

[7] J. Chapman "How Safe Is Your Data? Cyber-Security in Higher Education". HEPI Policy Note, **April 2019.**

[8] M. Whitman, H. Mattord, "Threats to Information Protection-Industry and Academic Perspectives: An annotated bibliography". J.Cybersecur. Educ. Res. Pract. **2016**.

[9] K.Beaudin," The Legal Implications of Storing Student Data: Preparing for and Responding to Data Breaches".New Dir. InstitutionalRes. **37–48, 2017.**

[10] K.Beaudi"College and university data breaches: Regulating higher education cybersecurity under state and federal law". J. Coll.Univ. Law 41, **657–693, 2015.**

[11] H.S. Hussain,R.Din,N.Z Khidzir, K.A.M Daud, S.Ahmad, " Risk and Threat via Online Social Network among Academia at Higher Education". J. Physics: Conf. Ser. 1018, 012008 , **2018**.

[12] I. Ajie, "A Review of Trends and Issues of Cybersecurity in Academic Libraries". Libr. Philos. Pract1–20. Available online:https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=5803&context=libphilprac (accessed on 28 January 2021).

[13] A.Diaz, A.T Sherman,A. Joshi, "Phishing in an Academic Community: A Study of User Susceptibility and Behavior". arXiv: 1811.06078, **2018**.

[14] T. Cuchta, B. Blackwood, T.R Devine, R.J Niichel , K.M. Daniels, C.H.Lutjens, S. Maibach, R. J Stephenson. "Human Risk Factors in Cybersecurity". In Proceedings of the 20th Annual SIG Conference on Information Technology Education, Tacoma, WA,USA, 3–5 October; **pp. 87–92, 2019.**

[15] M. Dadkhah, G. Borchardt, T. Maliszewski, ,"Fraud in Academic Publishing: Researchers Under Cyber-Attacks". Am. J. Med. 130, 27–30, **2017**.

[16] D. Teixeira ,J.Silva, A.Alkhatib, Tsigaris, P. "Spam emails in academia: Issues and costs". Scientometrics 122, **1171–1181, 2020.**

[17] G. Wangen, N. Hellesen, H.Torres, E. Brækken, "An empirical study of root-cause analysis in information security management ".In Proceedings of the SECURWARE-The Eleventh International Conference on Emerging Security Information, Systems and Technologies. International Academy, Research and Industry Association (IARIA), Rome, Italy, 10–14 September **2017**.

[18] H. Kashiwazaki, "Personal Information Leak in a University, and Its Cleanup". In Proceedings of the 2018 ACM SIGUCCS Annual Conference; Association for Computing Machinery: New York, NY, USA,; **pp. 43–50, 2018.**

[19] A.Deepa E. C. Blessie,"Input Analysis for Accreditation Prediction in Higher Education Sector by Using Gradient Boosting Algorithm", International Journal of Scientific Research in Network Security and Communication, **Vol.6, Issue.3, pp.23- 27, 2018.**

[20]A Survey on Impact of IoT Enabled E – Learning Services, International Journal of Scientific Research in Network Security and Communication, **Vol.6, Issue.2, pp.178-183, 2018.**

AUTHOR PROFILE

Ankita Sharma received the bachelor's degree in information technology in 2016 from Punjab technical university Jalandhar Punjab, India and recently working as the Assistant Professor. She has published more than 3 research papers in reputed international journals and it's also available online. Her research interest includes network security ,distributed network, cyber security and computer network, IoT and Computational Intelligence based education, Web Development.

