Overview of Cyber Security in e-Learning Education

Mridul, Rajiv kumar
Shobhit Institute of Engineering and Technology (Deemed to be University), Meerut
Email Id- mridul@shobhituniversity.ac.in, Rajiv.kumar@shobhituniversity.ac.in

ABSTRACT: ***The Internet's limitless area is referred to as cyberspace. The set of regulations put in place for the safety of this cyberspace is known as cyber security. Numerous studies have shown the growing usage of e-Learning systems, which continues to increase; nevertheless, little attention has been paid to the problem of e-Learning system security in both research and education. We provide a method to analyzing, assessing, monitoring, measuring, and controlling cyber security in the context of e-Learning systems in this article. Because e-Learning systems are accessed and controlled over the Internet by thousands of users across hundreds of networks, security is a unique issue. Furthermore, in light of their standard design and unique security needs, this study shows the frequency of internal cyber-attacks as well as a lack of appropriate IT policies and processes in e-Learning systems. We also go through the most significant security issues that may arise in distributed e-learning systems. Because e-Learning systems are open, dispersed, and linked, ensuring that only interested and authorized actors get access to the correct information at the right time is a significant problem.***

KEYWORDS: ***Cyber security, e-Learning systems, Cyber-attack, IT policies, Distributed e-Learning.***

1. INTRODUCTION

E-Learning is a popular form of learning that relies on the Internet to carry out its operations. E-learning systems exemplify the Internet generation's computer technologies and networks. These systems are complicated, and their goal is to ensure the learner's pleasure while also maintaining a positive picture of the learning process. There is strong evidence that new educational technologies, such as e-Learning, offer students, trainees, and instructors with unparalleled possibilities to learn, improve, and retain fundamental skills and knowledge. E-Learning systems, on the other hand, use the Internet to acquire all required information and expertise. Regrettably, the Internet has also become a hotbed for a new kind of criminal activity known as cyber-crime. Because e-Learning systems are open, dispersed, and linked, information associated with the e-Learning environment, some of which may be personal, protected, or private in nature, is constantly exposed to security risks. During the last several years, e-learning has exploded in popularity [1]. WebCT, Moodle, and Blackboard are examples of e-learning systems that are varied and widely used. They're big and busy, with a wide range of users and resources. Information sharing, collaboration, and interconnection are essential components of any e-Learning system. The data must then be safeguarded to ensure its confidentiality, integrity, and availability. In eLearning, data tampering, fraudulent user authentication, and confidentiality breaches are all major security concerns.

Meanwhile, e-Learning trends require that applications, learning environments, and heterogeneous systems be more interoperable. The goal of this article is to provide a high-level overview of the most pressing cyber security issues that affect Higher Education systems and future distributed e-Learning systems [1]. The next parts will address the following topics: cyber security and education; security risks, identification, and protection in distributed e-Learning systems; creating a security management model for e-Learning systems; and lastly, some conclusions. The use of information systems in higher education is rapidly being explored to fulfill the needs and expectations of diverse learners who want more than conventional classroom-based experiences [1]. Face-to-face components are being blended with e-Learning, Webinars, and other online digital material in new course delivery methods. Because there are possibilities for both synchronous and asynchronous interactions with online learning systems, building trust and promoting participation among users is critical. Synchronous learning takes place takes place in real time, with all participants interacting at the same time, whereas asynchronous learning takes place at a slower pace and allows participants to engage

in the exchange of ideas or information without relying on the participation of other participants at the same time [2].

1.1 Cyber security and education:

- Establishing digital credibility: Higher education is a completely different setting than it was a few years ago, and online learning technologies now provide substantial student involvement. Students are becoming more aware of information systems (IS) and information technology (IT) problems, therefore course providers' overall learning methods must be inextricably connected with IS/IT strategies in order to satisfy student requirements today and in the future. In terms of accessibility, security, and personal information protection, both digital natives and digital immigrants will have high expectations of their e-Learning system. This may involve the safe storage of a student's bank account information in connection with course fees and other purchases. Universities in the United Kingdom contain a large amount of intellectual property in the form of research and other academic resources, making them ideal targets for cyber-criminals. Researchers will expect their delicate work and commercially sensitive data to be safely kept, with no danger of theft or misappropriation. Institutions should do a cyber-security risk assessment and identify the optimal technology, personnel, and process configurations.
- Remote access and bringing your own device: Because the device is owned by the user rather than the data controller, bring your own device (BYOD) presents a variety of data protection issues. Students are comfortable utilizing technology for communication, information retrieval, collaboration, and as a learning and development platform. They also desire wireless and on-demand access to the university network, including any virtual learning environment, not just via the institution's own fixed PCs in designated computer rooms, but also through their own device (tablet, smartphone) from various on- and off-campus places. It is essential that the data controller guarantees that all personal data processing under his control complies with the Data Protection Act (DPA) of 1998. The DPA is founded on eight "good information handling" principles. These grant individual's particular rights over their personal information and impose certain responsibilities on the organizations in charge of processing it. Each organization's particular hazards will be addressed differently by a BYOD policy. Which personal data may be handled on a personal device and which must be kept in a more restricted setting is an essential issue to address. Universities and businesses should examine if students, professors, or workers who use their own devices are processing non-corporate data about the device's owner or other users. However, it is critical that users manage any relevant personal information in accordance with the DPA standards.
- Learning management system security: Current e-Learning systems that enable online collaborative learning don't fulfill all of the necessary security criteria . The majority of collaborative learning experiences are developed and executed with pedagogical concepts in mind, but security concerns are often overlooked. Students falsifying course assessments, presenting a convincing false identity to others, intrusion into controlled or private conversations, alteration of date stamps on submitted work, and a tutor gaining access to students' personal data are all examples of undesirable situations that have a negative impact on the learning process and its management. Using a Public Key Infrastructure (PKI)-based approach to provide essential security properties and services in online collaborative learning, such as availability, integrity, identification and authentication, access control, confidentiality, non-repudiation, time stamping, audit service, and failure control. PKI presupposes the usage of Public Key Cryptography, which is the most widely used technique for authenticating a message sender or encrypting a message over the Internet. For the encryption and decryption of communications, traditional cryptography has typically required the production and distribution of a secret key. This private key method has the major drawback that communications may readily be decoded if the key is found or intercepted by someone else. As a result, on the Internet, public key cryptography and public key infrastructure are the favored methods.
- Higher education faces the most serious cyber security risks: The passionate and early adopters of technology are using mobile devices, with new gadgets permeating campuses throughout the nation. Every day, a slew of new and sophisticated mobile devices (such as iPads, new Android phones, tablet

devices, and portable Internet access systems) are released with updated operating systems, making them ripe for infection and ready to attack a university's network system. It's therefore crucial to support these devices while keeping a full picture of their connection and interactions with the university system.

- Viruses and Social Media: Students in universities and colleges are the most active users of social media sites such as Facebook, Twitter, and YouTube. This will allow Malware and other infections, such as Wildfire, to be hosted and distributed via social networking platforms. On a college or university campus, permanently blocking access to social media will be almost difficult. In order to maintain network security and safeguard critical data, it's critical to quickly identify compromised devices.
- Desktop to server virtualization: Virtualization is a widely utilized and popular technique in many kinds of businesses, including higher education institutions. The system allows for substantial hardware and administrative cost reductions, as well as the adoption of a green approach and the use of virtualized desktops. More risks will emerge as more people migrate to virtualized settings. Higher education institutions must remember that hosted virtualised desktops (HVDs) should be treated the same as conventional devices, since they pose the same risks.
- IT's Consumerization: Users who purchase their own devices, utilize their own personal online service accounts, install their own apps, and then connect to the university or corporate network with the device - sometimes without the knowledge or permission of the organization - are driving IT consumerization. The issue has become much more difficult to handle in the Higher Education sector due to an institution's own consumerization of IT. Higher Education institutions will face greater network security risks as users increasingly utilize their own devices for professional purposes. In reality, the consumerization of IT is increasing the need for network security solutions that can protect a variety of devices and infrastructure components. Regardless of the kind of device or location, security solutions that detect every consumer-adopted device, scan for risks and inadequacies, and then provide access or automatically repair issues are required [3].

1.2 Security threats, detection and protection in distributed e-Learning systems:

E-learning systems have the same features and difficulties as other e-services in that they need information exchange and dissemination. They are linked to the accessibility of services through the Internet, a person's consumption of services via the Internet, and a customer's payment for a service via the Internet. Organizations must place a higher focus on security risk management, taking into account the many threats and vulnerabilities, as well as the various interactions and integration between clients, servers, databases, and other components [4].

- Issues with cyber security in distributed e-Learning systems: Software assaults (viruses, worms, macros, denial of service), espionage, acts of theft (illegal equipment or information), and intellectual property theft are all significant security risks to E-systems (piracy, copyright, infringement). E-Learning systems offer several unique characteristics, such as a wide range of users, numerous applications, and data to download and upload. E-systems are susceptible to a variety of security risks, as summarize:
- Authentication - insecure communication due to failed authentication and session management.
- Availability – service denial
- Unsecured encrypted storage; insecure direct object reference; information leaking; and poor error handling are all examples of confidentiality threats.
- Buffer overflows, cross-site request forgery, cross-site scripting, failure to limit URL access, injection vulnerabilities, and malicious file execution are all examples of integrity threats.

A threat is a kind of item, person, or other entity that poses a threat, such as Trojan horses or phishing. Password-based authentication schemes are particularly vulnerable to phishing attempts, which are getting more complex and require robust preventive and responses [12]. have also proposed and demonstrated the use of a Mean Failure Cost (MFC) model for managing and quantifying security threats, paying particular

attention to the following: the basic architectural components of an e-learning system; the various stakeholders; the various security requirements; and the various types of security threats.

- E-Learning Privacy Issues: May and George recognize the technological and ethical challenges of employing a tracking system to monitor and analyze the many human-computer interactions that occur in computer mediated learning (CML) in e-Learning, distant learning, and blended learning. They've increased awareness of security and privacy as critical concerns for practitioners and academics that use student monitoring and personal student data. Participants will be better able to avoid security risks and protect themselves and their learning settings if they have a better knowledge of the problems. The virtual learning environment's suppliers, as well as the instructors who distribute the material, are concerned with providing a secure learning environment and the safe preservation of private student data. Learners themselves assess the learning environment's trustworthiness and are concerned about the security of their sensitive personal data. Data gathered on privacy and security concerns in technology-enhanced learning revealed that individuals ranked the following elements in order of decreasing importance: Awareness raising > data protection > learning resource authenticity > seamless access > address and location privacy > single sign-on > digital rights management > legislation > anonymous usage

1.3 Developing a security management model for e-Learning systems;

As part of their current governance frameworks, higher education institutions should adopt corporate methods to manage their information security risks. In order to create clear lines of information in an institution that shares safely in a dispersed environment, institutions must first define the data 'controls.' Implementing cyber security governance requires a thorough knowledge of the risks that the institution faces and the safeguards in place. It will require daily accountability for risk assessment, management, and reporting. Heads of schools, principles, the academic staff, and the IT group at a higher education institution should be well-informed about their duties and vigilant about changing threats and dangers to data users. The process model created for handling cyber security risks in higher education [5]. All higher education institutions should be aware of their responsibilities for the security of institutional and research data and put in place adequate safeguards to guarantee compliance with the Data Protection Act (1998) [6]. Most higher education institutions will have various data and research management systems in place, as well as appropriate degrees of supervision. The majority of these organizations and researchers will have a wide range of data management rules and procedures in place, with little regard for mistakes. These characteristics make it difficult for corporate governance to comprehend both the problems and the need for an employee cyber security threats process model. Ultimately, network security is a shared responsibility for the whole organization. By exchanging information with peers and government officials, network administrators and defenders may keep up to current on risks and countermeasures. The users, who are critical to the security of any network and information, are much more essential. They must play a key role in assessing the danger that information poses, setting security priorities, and, ultimately, implementing safeguards as users [7].

2. LITERATURE REVIEW

[8] Propose that The Internet is becoming increasingly interwoven in the daily lives of many individuals, organizations and nations. It has, to a large extent, had a positive effect on the way people communicate. It has also introduced new avenues for business; and it has offered nations an opportunity to govern online. Nevertheless, although cyberspace offers an endless list of services and opportunities, it is also accompanied by many risks, of which many Internet users are not aware. As such, various countries have developed and implemented cyber-security awareness and education measures to counter the perceived ignorance of the Internet users. However, there is currently a definite lack in South Africa (SA) in this regard; as there are currently, little government-led and sponsored cyber-security awareness and education initiatives. The primary research objective of this paper, therefore, is to propose a cyber-security awareness and education framework for SA that would assist in creating a cyber-secure culture in SA among all of the users of the Internet. This framework will be developed on the basis of key factors extrapolated from a comparative analysis of relevant developed countries.

[9] Propose that The usage of personal online banking and E-commerce is quickly growing as a result of the recent growth of the internet. Furthermore, services and marketing in companies, governments, and banks are quickly expanding, mostly via online shopping malls and websites. As a result, cyber assaults such as clever and high-tech APT attacks, cyber infiltration access, and digitalized information are on the rise. Countermeasures, operation drills, and security education regarding these security incidents, on the other hand, are not carried out effectively. As a result, the goal of this research is to create an internet-based cyber information security training system. In addition, in order to cope with security incidents caused by malicious emails and attachments, which are common at public institutions and private businesses, information security education is being tested out on connected workers as well as education and training topics utilizing the system. By avoiding information loss or a computer system's paralysis, security incidents caused by phishing emails may be avoided in advance, and economic losses could be reduced.

[10] Propose that The complex global internet environment, in addition to presenting us with many possibilities, also poses a number of cyber security problems. Designing and implementing up-to-date cyber security education is one of these difficulties. After being tasked with developing an MSc program in cyber security for professionals, we quickly found that the scientific body of knowledge that underpins such a curriculum is not readily accessible in an organized format. As a result, we were compelled to construct the software by combining data, expertise, and methods from a variety of scientific fields and cyber sub-domains. We provide our results in this article by (a) sketching the selected conceptualization of cyberspace and its security issues, (b) the rationale for adopting an integrated cyber risk management strategy, and (c) the resultant profile and general set-up of the program. Our efforts also yielded a slew of fresh discoveries. We demonstrate the latter by describing our novel cyber security risk management methodology, which is a fundamental expansion of current popular information security risk management methods.

3. DISCUSSION

As the internet's reach grows to include increasingly wider areas of our economic and social well-being, cyber security is becoming a significant worry for academics and practitioners, including issues such as privacy, confidentiality, and user identification. Because they include many stakeholders, geographically dispersed resources and data, and specific needs for secrecy, authentication, and privacy, e-learning systems epitomize computer systems and networks of the internet age. The Mean Failure Cost for E-learning Systems is shown in this article as a rigorous cyber security metric of dependability to quantify security risks. The suggested architecture enables an analyst to assess a system's security in terms of the loss that each stakeholder would suffer as a consequence of security failures. We've also improved the methodology to account for important security needs. Our primary goal is to provide a diagnosis of potential issues with non-secure systems, as well as a deep understanding of critical needs, critical risks, and key components of the cyber system. This enhancement is advantageous and offers up a broad variety of options for future economics-based research.

4. CONCLUSION

Higher Education's main business of delivering courses to different learners has altered as a result of the need for e-Learning. Organizations must seek out and implement innovative services that will allow students to learn successfully and safely in a virtual setting. Higher Education IT departments are finding it more difficult to retain control over how data is utilized, saved, and shared within and outside the virtual class due to increasing demand from e-Learners for flexibility, mobility, and empowerment. Building safe, consistent, highly accessible e-Learning environments, as well as centralized application administration, is required for the deployment of new services to satisfy demanding user requirements.

REFERENCES

[1] M. Aparicio, F. Bacao, and T. Oliveira, “Grit in the path to e-learning success,” *Comput. Human Behav.*, 2017, doi: 10.1016/j.chb.2016.10.009.

[2] M. Ramim and Y. Levy, “Securing e-learning systems: A case of insider cyber attacks and novice IT management in a small university,” *J.*

Cases Inf. Technol., 2006, doi: 10.4018/jcit.2006100103.

[3] Y. Ban, K. Okamura, and K. Kaneko, "Effectiveness of Experiential Learning for Keeping Knowledge Retention in IoT Security Education," 2017, doi: 10.1109/IIAI-AAI.2017.206.

[4] Y. Levy, M. M. Ramim, and R. A. Hackney, "Assessing ethical severity of e-learning systems security attacks," *J. Comput. Inf. Syst.*, 2013, doi: 10.1080/08874417.2013.11645634.

[5] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *Comput. Secur.*, 2013, doi: 10.1016/j.cose.2013.04.004.

[6] E. T., R. Y., and S. D., "Barrier Free Internet Access: Evaluating the Cyber Security Risk Posed by the Adoption of Bring Your Own Devices to e-Learning Network Infrastructure," *Int. J. Comput. Appl.*, 2017, doi: 10.5120/ijca2017915581.

[7] T. Limba, T. Plėta, K. Agafonov, and M. Damkus, "Cyber security management model for critical infrastructure," *Entrep. Sustain. Issues*, 2017, doi: 10.9770/jesi.2017.4.4(12).

[8] N. Kortjan and R. Von Solms, "A conceptual framework for cyber security awareness and education in SA," *South African Comput. J.*, 2014, doi: 10.18489/sacj.v52i0.201.

[9] B. H. Kim, K. C. Kim, S. E. Hong, and S. Y. Oh, "Development of cyber information security education and training system," *Multimed. Tools Appl.*, 2017, doi: 10.1007/s11042-016-3495-y.

[10] J. Van den Berg *et al.*, "On (the emergence of) cyber security science and its challenges for cyber security education," *NATO STO/IST-122 Symp. Tallin*, 2014.