Best Practices for E-Learning Systems to Deal With Cyber Threats

Pranay Chauhan, Dr. Jayshri Bansal

Trainer, BDM, Prestintech Pvt Ltd

Assistant Professor, Human Resource Development Center, Devi Ahilya Vishwavidyalaya, Indore.

Abstract: Virtual education is being used to describe a modern type of user training. In contrast to the conventional teaching approaches, it facilitates awareness for consumers not just for schools, but also for the organizations. E-Learning is implemented in the sense of schooling, including continuing study, company training, student training, and so on. Online education is "a form of the system of distribution used in remote teaching that permits a coordinated and simultaneous contact channel sharing of resources." It stores information using Content directories and uses technologies to assist students interact with teachers and others. Online education began as an online and Web-based learning tool to carry out training. Nevertheless, certain criminal acts are taking place,and vulnerabilities exists on the network. Therefore, the e-learning world eventually faces persistent challenges, hazards, and challenges in the field of defense. Sadly, many public universities scramble into implementing online educational structures without consideration and deep knowledge of digital ensuring safety. This whole paper aims to integrate this knowledge and enable online education executives and operators to recognize the state-of-the-art in this rapidly changing area. E-learning is a virtual or interactive learning tool relating specifically to the Internet in its implementation as a modern means of study. Inherently, the Web is vulnerable as the core of every program. Owing to the other benefits, such as decreased prices, quicker deployment, efficient learning, and reduced ecological consequences, multiple companies are utilizing online learning without much concern for health and safety. Nonetheless, a well-protected atmosphere is needed for the e-learning program to operate. E-learning protection is a crucial factor in maintaining an efficient online content distribution.

***Keywords*–Education, MOOC, Attacks, Cyber defense.**

I. INTRODUCTION

Online Learning Program also provides an interactive world for consumers and teachers with the use ofdatabase in apps and software. Interactive technologies give consumers and administrators many benefits including unified data collection, opportunities for students and educators, and simple tracking. Also, facilitates users to conveniently link to them easily and access them quickly, all records, content (eBooks, images, messages, photographs, etc.) are firstly stored on the web. Of starters, certain computing tools such as tablets, computers, or handheld devices can be used by consumers. Deviceswith strong internet access can subscribe to the websites instantly and conveniently and take the advantages of online courses. Secondly, for students and instructors, the simulated world often provides certain advantages [1].Learnerswill access these resources from anywhere. Students will access and submit their assignments to their instructors. Instructorswill submit assessments, homework, build courses, collect inputs, and would be able to easily give feedback to their students. All e-learning services would be held in one location on a site thus, instead of tracking the data from various places, the administrator will access all sorts of data [2]. E-learning relies entirely on the internet to exchange and reveal knowledge like every other e-system. Inherent protection risks include assaults on the database, software, malfunction of the program, and property rights vulnerabilities (licensing, fraud, violation), which are the foundation of an e-system. Sadly, too little has been achieved to fix this problem. Trustworthy operating frameworks will no longer be built for open networks without considering malicious threats. In order to promote the protection of decentralized technology systems, program developers and device builders will be conscious of future approaches on the horizon [3].

Online education security relates to electronic learning defense from harmful or unintentional usage. Data privacy is the protection of confidential details against unwanted access as well as from the avoidance of illegal divulgation of knowledge. Protection includes three basic requirements: Confidentiality, completeness, and availableness. As there are significant number of participants(including guests, teachers, tutors, and administrators) in any online education area, either a log-in framework or a strict boundary marking is required to guarantee that only verified users access authorized sites. Safety is critical for maintaining the consumers' data in the online learning environment since any danger will significantly affect student's perception on the reliability and credibility of the program. Consequently, it is important to know the causes causing protection challenges in online learning and to recognize the shortcomings of the existing case of any concerns. Defend-measures could then be established to reduce online education safety risks. Safety protections such as data encryption are typically introduced to secure sensitive details. Integrity, a major security component, relates to the safeguarding of data against unauthorized or intentional changes and the lack of improper system modification.

II BACKGROUND

Pros of Online Learning:

a. **Anytime learning:**

On-line programs provide exceptional flexibility, mainly for college learners who are already balancing a full-time career, wanting to acquire new skills beyond their field or vocational professionals. Professionals learners can opt do it after work or even during the lunch hour wheneverpreferred.

b. **Learning at your pace:**

Most participants are not confident in lifting their hands in the classroom and hesitates in calling the instructor to explain a question already understood by their classmates. In online learning, you can pause/ interrupt videos andrefer tothe previous modules’topics[4].

c. **Cost-Effective:** Few universities offer free/ reduced fee courses as infrastructure costs like room and board costs, and other transportation expenditures will be reduced. And as more autonomy occurs, salary and employment are possible at the same time [5][6].

d. **Geographical boundaries may be broken:**

With online system you are not restricted by the geography. We can engage in the community lessons with other students around the world. Through interacting alongside individuals from diverse cultures and nations, you will develop a regional outlook and learn to collaborate – few good qualities managers seek in applicants.

Cons of Online Learning:

a. **Interaction with Professors:**

Users will have restricted contact with teachers based on the type of online curriculum you select. Professors can address your concerns and plug the gap, but you mustconsider the level of faculty participation that you have to feel as if you are progressing.

b. **Fewer possibilities for networking:**

There might be limited chances for networking with classmates based on the course you choose. If the social factor is essential for you, choose an online learning platform that focuses on peer active participation engagement, or even provide activities.

c. **Cannot be destabilized:**

To complete an online course, time and self-discipline are required. Since you don't have to prepare and operate on fixed days in a week, it's up to you to set aside time to research. You can excel in an online community if you are strongly structured and are willing to adhere to a timetable.

Opportunities in Online Learning:

Digital starting to learn promise lies in three components: Flexibility, Interconnectivity, Collaboration.

a. **Flexibility:** Freedom of movement is a prime chance for online learning. For e.g., the conventional learning environment depends heavily upon paper-based resources.

b. **Interconnectivity:** Interconnectivity and online learning are different problems, but online learning experiences may be interactive, which implies that the teaching method enables students and participants to actively interact with artifacts in the online environment[7].

c. **Collaboration:** Whereas interconnectivity mainly deals with experiences with the learning environment, teamwork encourages students to work with other students in a specific project or activity that is difficult for a person alone to accomplish.

Challenges in Online Learning:

Online learning has looked at patterns and potentials and we express obstacles that we consider with the growth of online learning.

a. **Distribution of resources:**

Developers are becoming gradually conscious of the various meanings of online education: from CD-ROMs to web-based apps, etc. There appears to be constant reference to the means of distribution. One reason is that commercial people are typically driven to sell their products.

b. **Innovation vs. Dedication:**

Online education tends to be an area of growth. Methods like learning analytics are continuously evolving in the learning phase. A quality experience makes it appear on the market before the educational establishment can comfortably decide to commit to a system. The choice to stick to a program is also a tough one.

c. Intellectual rights and ownership:

Copyright is also a major challenge for online education. The entire nature of the Internet is like the reverse of patents and creative assets. The Internet is to be exchanged. They continuously need exposure to current works of curriculum, bethey books, pieces of art, etc[4].

Cyber-attacks in education:

a. **Distributed Denial of Service (DDoS):**

Connections to and information within a school district will be withheld on a day-to-day basis. DDoS targets an infrastructure with junk mail, relevant data, and so on flooding the platform. Using antivirus and firewalls will reduce the likelihood of a DDoS threat. Frequent penetration checks can find potential holes in the university programs.

Table 1: Type of Attacks

Sno	Type of Attack	Payload	Damage
1	Malware	Malware injection	Intruder can access control over system
2	Ransomware	Malware, Ransom	Demand ransom, financial loss, Data can be encrypted
3	Phishing , Spear Phishing	Emails, Phishing Websites	Intruder can access control over system
4	Identify theft	Vulnerable os	Loss of personal data
5	Distributed Denial of service attack	Flooding Data packets	Denial of service
6	Password Attack	Brute forcing	Personal Data can be loss

b. **Malicious software:**

Ransomware, bugs, worms, and adware are known as malware. It is recommended to require students to be equipped with up-to-date anti-malware before connection to the university network. Malware may lead to theft, fraud, or operational activities being halted.

c. **Phishing:**

Another challenge faced by universities is the possibility of exposure of legal university email accounts in the wrongful hands. They formulate similar email accounts and links duping learners to click these links which enable these malicious user to access university's entire email server.

d. **Unprotected personal equipment:**

Each participant has a smartphone and a notebook at minimum, to not include exercise tracking or laptops. The more gadgets the greater the network's weakness. Controls are carried out and danger analyses are conducted periodically to protect the wireless connection.

Actions to adopt a successful system of data security:

a. Build an organizational security group:

The very first move toward building up an information security policy is to build the organization's security leaders. The perfect group consists of a supervisory board that drives the plan and sets the goals and an interdepartmental division that performs.

b. **Recognize data assets:**

A central registry of all knowledge assets held by the company, including resources from third parties, is the next big move in the declaration of ownership.

c. **Evaluate all infrastructures:**

Multiple universities have been affected by unpredicted attacks because of lack of planning. Tracking applications over communication networks will ensure no inappropriate events arise.The standard method is to identify the necessary incident management techniques during all involved phases, including a technical support method for logging incident tickets and assigning consultants.

d. Analyze the potential protection positioning:

Upon defining and categorizing all communication properties, an in-depth review of possible threats and weaknesses will be carried out.

e. **Vulnerability management:**

The next priority will be given to the vulnerability and weaknesses based on chance and future effects. Risk management in addition to the existing measures taken to prevent such risks, usually a comprehensive risk assessment exposes all existing weaknesses [8].

f. **Share information and direct preparation:**

The performance of the entire protection project is ensured by daily instruction and education practice with all the stakeholders.

g. **Secure all gadgets with powerful authentication:**

Don't neglect to protect the details and don't exchange knowledge with colleagues or other workers. Keep your credentials secure and update them frequently with complex combinations [9].

h. **Keep upgrading the device:**

For your operating systems and internet protection tools, this is particularly relevant. To bypass your network, cybercriminals also use the identified bugs or vulnerabilities in your program.

i. **Enable the firewall:**

Prevent access of unauthorized or fake domains and avoid other kinds of malware and hackers. A firewall is cybersecurity in the foreground.

j. **Use malware/anti-virus software:**

Impede viruses by downloading and routinely saving virus protection from infecting the device.

k. **Safe smartphone devices:**

Stay aware of the susceptibility of your electronic computer to malware and hackers. Install proprietary software.

f. **Share information and direct preparation:**

The performance of the entire protection project is ensured by daily instruction and education practice with all stakeholders.

Conclusion:

Recently there is a shift in trend and teaching & corporate organizations have started preferring E-learning ways over conventional classroom learning. Online education has its many advantages which we discussed in detail above. But it has its share of challenges like availableness and data confidentiality & security. There would be a need for a solid defense mechanism in place since we will have all the data on the internet including consumers' information, training material and all the course artifacts. One needs to consider all above discussed best practices and security measures while adopting e-learning. All these practices would ensure data confidentiality and would reduce the risks of cyber threats.

References:

1. Rjaibi, N., Rabai, L.B.A., Aissa, A.B., Louadi M.: Cyber Security Measurement in Depth forE-learning Systems. International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, No. 11, 1-15. (2012) 14.

2. Hashemi, S., Hashemi, S.Y.: Cloud computing for E-learning with more emphasis on security issues. International Journal of computer, electrical, automation, control, and information engineering, Vol. 7, No. 9, p.8. (2013)

3. Arkorful, V., Abaidoo, N.: The role of e-learning, the advantages and disadvantages of its adoption in Higher education, International Journal of Education and Research, Vol. 2, No. 12, 1-14. (2014)

4. Derntl, M.: The Person-Centered e-Learning pattern repository: Design for reuse and extensibility. In: Proceedings of EDMEDIA'04 - World Conference on Educational Multimedia, Hypermedia & Telecommunications, pp. 3856--3861. (2004)

5. He, W. (2012). A review of social media security risks and mitigation techniques. Journal of Systems and Information Technology, 14(2), 171-180.

6. He, W. (2013). A survey of security risks of mobile social media through blog mining and an extensive literature search. Information Management and Computer Security, 21(5), 381–400.

7. Borstorff, Patricia C, and S Keith Lowe. "Student perceptions and opinions toward e-learning in the college environment." Academy of Educational Leadership Journal, Vol. 11, No. 2, 2007, pp. 13-128.

8. Aggarwal, A. K. (Ed.). (1999). Web-Based Learning and Teaching Technologies: Opportunities and Challenges: Opportunities and Challenges. IGI Global.

9. McMahon, J. D. (2007). Ethical issues in web-based learning. Flexible Learning in an Information Society, 209.