ISSN 2047-3338

Security Threats and Remedies in E-learning System

Ms. Aakanksha Chopra[1] and Ms. Ankita Chopra[2]

[1,2]Jagan Institute of Management Studies, Affiliated to GGSIPU, Dwarka Sector-16C, Delhi, India

[1]aakankshachopra.spm@gmail.com, [2]ankita.chopra@jimsindia.org

***Abstract*— E-Learning can be defined as the use of available information and communication technologies to facilitate learning process. E-Learning is the combination of learning and the Internet technology. In the modern world, education has become more global, and people are looking for learning with ease and interest. Through this paper, we will understand and discuss how e-learning systems can provide quality education and also discuss security threats and remedies in the E-learning system. We will all focus on harmful E-Threats, E-Risks, how e-threats leads are dangerous to assets and will also discuss various e-remedies to avoid all the E-Threats. We will also understand six categories of information security threats to our E-learning system by STRIDE model**.

***Index Terms*—E-Learning, Education, E-Threats, Assets, E-Risk, E-Remedies and STRIDE Model**

I. INTRODUCTION

E-LEARNING can help produce positive outcomes; research also seems to indicate that a more technology-rich environment delivers greater impact. Now that affordable e-learning solutions exist for both computers and internet it only takes a good e-learning tool for education to be facilitated from virtually anywhere. E-learning offers the ability to share material in all kinds of formats such as videos, slideshows, word documents and PDFs.

Be it yesterday, today or tomorrow the trepidity of security breach will always remain a threat. Where there is information there is always ways and methods by which that information can be snitched. The problem is not of data getting snitched the problem is the malicious sources behind this are some trusted people from within the organization. *Elliot Masie* once said, "We need to bring Learning to people instead of people to learning". E-Learning in recent years has reached a new ladder to success by getting all the professional, academicians, trainers, students or even kids together. E – Learning has all together embraced the virtue of the internet to create an online education the embarking industry. E-learning has taken control over this multi-device world and education is insuperable as it has crossed all the barriers today. Be it any medium learning, education, innovation is traveling miles by E-learning systems. They are not restricted by any locality, treasure, time, generation or prominence.

E-learning system is entirely based on the Internet and the information on the internet is continuously exposed to the security threats [6]. The concept of this paper is to understand E-learning system and security threats to ensure safety and security of information and learners private data.

Ms. Aakanksha Chopra (Assistant Professor (IT)) is with the Jagan Institute of Management Studies, Affiliated to GGSIPU, Dwarka Sector-16C, Delhi, India, (Email: aakankshachopra.spm@gmail.com)

Ms. Ankita (Assistant Professor (IT)) is with the Jagan Institute of Management Studies, Affiliated to GGSIPU, Dwarka Sector-16C, Delhi, India, Chopra (Email: ankita.chopra@jimsindia.org)

II. LITERATURE REVIEW

A) The impact of e-learning

The potential of e-learning to significantly affect education in developing countries is thus significant. Identifying the actual impact that e-learning programs have had on students, schools and their countries is, however, difficult. Because of the newness and diversity of the programs and the complexity of factors affecting outcome, measuring e-learning's impact is an emerging science. Nevertheless, some direct and indirect outcomes can be discerned.

They are presented below by e-learning's impacts on students, teaching, the economy and lastly on society.

1). The impact of e-learning on student achievement is complex and mediated by a range of other factors affecting achievement. It is clear, however, that:

a. Their effectiveness is closely related to how the technology is used as an educational tool. Students learn best with e-learning when interactively engaged in the content. Using technology can motivate students, particularly underachieving students, to learn.

b. Teachers report that tutorials in subjects such as math and science significantly improve student performance. Word processing software improves writing skills.

c. Providing technology on its own has little impact on achievement. Substantial effort must be put into

infrastructure, teacher training, curriculum development, assessment reform, and formative evaluation.

2). The effect of e-learning on teachers and teaching parallels that of students. It includes:

a. The pedagogy often shifts from a teacher - centered classroom environment to a more learner - centered environment, allowing more effective use of technologies.

b. Teachers report that they gain confidence, self-esteem and renewed motivation in e-learning environments.

c. There are significant barriers to teachers in developing countries that need to be overcome including their lack of ICT skills and ICT-related pedagogical skills.

3). The economic impact of e-learning can be examined by first, identifying the impact of e-learning and improvements in education on the workforce and employment, and second, the effect of a high tech workforce on the national economy.

a. An improvement in education positively affects economic growth, both in terms of an increase in GDP and an increase in income for workers. This is clear in both developed and developing countries.

b. As technology and knowledge spillovers are the foundations of modern economic growth, it is important to ensure that the workforce has the skills to meet the need of these 21st Century jobs.

c. The average increase in annual income for each additional year of schooling, especially secondary education, for an individual is 10%. The affect is stronger in developing countries than in developed countries.

4). The impact on society of e-learning programs is similarly difficult to separate out from the multitude of other factors affecting society. The potential impacts of e-learning— providing underserved-groups access to quality education, for example, can be important. What is known about the impacts in developing countries include:

a. The "digital divide" between those people and countries with access to digital technologies and those without, is narrowing as information and communications technologies become increasingly available and less expensive. African countries are catching up fast, but from a lower base than other developing countries. Some of the widest digital divides are within countries: between rural and urban centers, and between rich and poor communities. This is unfortunately parallel to statistics of student enrollment in secondary schools. e-Learning has the potential to address this gap by bringing quality education to rural and other underserved schools, but poor infrastructure and other challenges are greater in those areas than in the better served urban areas, and experience to date is that these areas are underserved with e-learning as well; e-Learning programs that overcome these challenges thus have the potential to have large impacts on learning.

b. e-Learning technologies could potentially play an important role in reducing the gap in access to education and in achievement by girls and other underserved communities in developing countries. Currently, the gap in access to education of girls and underserved students is mirrored by a gap of them using the Internet and other ICT technologies, partly due to societal norms and partly due to their economic situation. Introducing e-learning technologies into schools can assist girl and other underserved students improve their ability to participate and thrive in schools. Governments and international organizations are designing e-learning programs to deliberately address the gender gap.

c. Language proficiency can be an impediment for students and teachers to take full advantage of e-learning's benefits. Off-the-shelf educational software and most websites are in English or another global language, and students in Tanzania and vi Analysis of e-Learning elsewhere whose main language is not a global language may need to become proficient a second (or third) language. The ubiquity of English on the Internet has been found to be a strong motivator for young people in many countries to learn English. In schools where a global language is not the language of instruction, however, it is important to customize educational software. d. The prevailing pedagogical culture in countries mediates how e-learning is adopted. In Eastern countries, for example, e-learning approaches run against educators' preferences for expositive teaching and authoritative delivery, in which case computers are simply used to deliver content. The potential transformative role of e-learning to develop 21st century skills in many countries may require, thus, integrating e-learning into the system from curriculum development to teacher professional development.

B) Security aspects of e-Learning systems

It represents a unique challenge as numerous systems are accessed and managed via the Internet by thousands of users over hundreds of networks. E-Learning has gone through a spectacular development during the past years. E-Learning systems are diverse and widespread, with examples including WebCT, Moodle and Blackboard. They are large and dynamic with a variety of users and resources. The sharing of information, collaboration and interconnectivity are core elements of any e-Learning system. Data must then be protected in order to maintain confidentiality, integrity and availability. Protecting against data manipulation, fraudulent user authentication and compromises in confidentiality are important security issues in eLearning. Meanwhile, e-Learning trends are demanding a greater level of interoperability for applications, learning environments and heterogeneous systems.

C) E-Threats

E-learning system has helped all people be it rich or poor, lacking in time, money or resources to come on a common platform INTERNET and "learn." These new inventions have actually made learning a child's play. From no access to easy access towards learning, we are making E- learning system *"The next future of education."* The biggest threat is how to deal with Author, Teacher, Manager, System Developer's and Students Risk? [4].

E-learning system is an online system which is prone to computer threats. E-threat leads to E-risk. Bandara, Ioras, and Maher [3] have stated that *Risk is* the probability of the occurrence of a particular *threat* and expected loss. For example we can say that E-risk is a risk involved at the time of electronic transfer of money or giving bank details for

online transactions, moreover, threat means predicted vulnerabilities.

Alwi and Fan [1] have explained and reviewed the security issues which may occur in E-learning system. They have broadly categorized various threats. Table 1 describes various security threats and categories of E-Threats.

Table 1: Security threats and categories of E-threats

Various Serious threats	Categories of E- threats
Worms, macros, denial of service	Deliberate software attacks
Bugs, programming errors, undetected loopholes	Technical Software failures and errors
Employees mistakes, accidents	Acts of human error or failure
Unauthorized access, data collection	Deliberate acts of espionage or trespass
Destruction of information or system	Deliberate act of sabotage or vandalism
Equipment failure	Technical hardware failures or errors
Illegal confiscation of equipment or information	Deliberate acts of theft
Privacy, copyright, infringement	Compromises to intellectual property
Power and WAN service issue	Quality of service deviations from service providers
Antiquated or out-dated technologies	Technological obsolescence
Blackmailing for information disclosure	Deliberate acts of information extortion

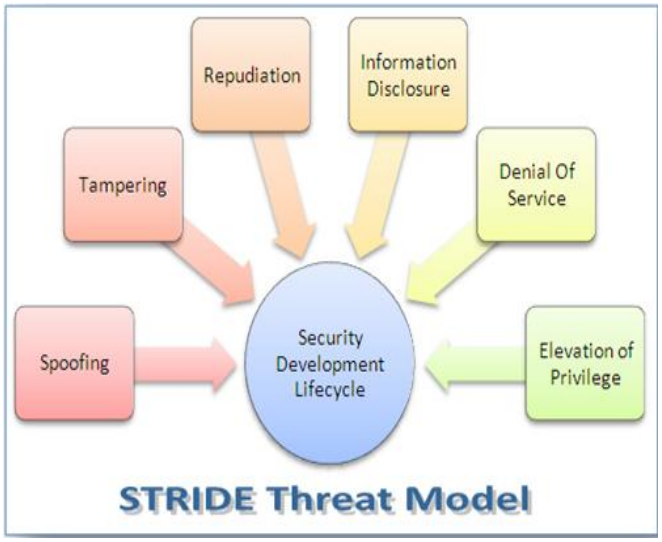

Fig. 1: STRIDE Threat Model

Our E-Learning systems are open, distributed, interconnected and most importantly are susceptible. We need to take security measures to foster our E-Learning systems and all the assets. According to [2], Assets are valuable resources of an organization that needs to be protected. Any loss of the assets is loss to that organization. Assets can be users, servers, services, information networks, documents, goodwill, personal skills etc.

The eminence of the E-Learning system is that learners are able to learn from it in real-time. This system is live and dynamic in nature hence highly vulnerable and sensitive in nature. Today, looking at the information getting ruptured at an extremely high velocity it has become very important to detect all the threats towards the system and rectify them. We need to analyze and identify the amount of upcoming risk in such a way that we should try to reduce the level of risk to an acceptable level; this can be done by *Risk Management Process* [2]. It states that the evaluation of risk on assets, threats and vulnerabilities are done in assessment phase.

Zamzuri, Manaf, Ahmad, and Yuzaimi stated in [7] that assets take services provided by the e-learning system such as learning resources, examination or assessment questions, students' results, user profile, forum contents, students' assignments and announcements in the e-learning system.

STRIDE model also known as STRIDE security model is a system developed by MICROSOFT for computer security threats, see Fig. 1. STRIDE model was given to classifying scheme for characterizing known threats by intruders and malicious users of the system and the information [10].

i). *Spoofing Identity:* is a method by which user's data is accessed in an unlawful manner and is used against that user for authentication purpose. The information of the user like username, passwords, OTP's is used. Basically, malicious users try to become an authentic user illegally which they are not in reality.

ii). *Tampering with Data:* Modifying the data viciously. They try to change persistent data that appears in the database. They also fling to alter the data that is flowing between two systems in an open network such as Internet. By doing this they try to swing client-side validations- GET and POST results, HTTP header, cookies etc.

iii). *Repudiation:* This kind of threat is faced when users deny of transferring a disputed transaction when other parties are not having any proofs of the transfer and lacks in the ability to trace it. Nonrepudiation refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package.

iv). *Information Disclosure:* Disclosing private details to individuals and systems leads to the leak of information. It gives green signals to intruders to read and access and misuse that file that they were not granted access to. Sometime the intruders also extract this type of information like passwords while two computers are sharing information.

v). *Denial of Service (DoS):* This type of attack has crossed heights. DoS attacks refute services to authentic users' like- making a webpage temporarily

unavailable or unusable. This type of attack reduces system availability and reliability to a great extent.

vi). *Elevation of Privilege:* This is one of the most dangerous situations as in this type of threat, an unprivileged user gains privileged access to the system. Thereby they have sufficient access to compromise or destroy the entire system. It includes situations in which an attacker has effectively penetrated all system defences and become part of the trusted system itself.

Zamzuari, Manaf, Yunus, Ahmad in [5] depicted, surveyed and concluded all the six STRIDE components and gave a result as, "Critical level of e-learning services" and "Critical Level of e-learning security components".

III. E-REMEDIES

E-learning security is the process of preventing and detecting the use of your computer system [6]. In this section, we will be discussing about E-Remedies for all the threats and risk with e-learning system. Following are various techniques or tools that can be used to protect information and system against all the threats.

i). *Controlling Access using Firewalls:* A firewall is a hardware device or software system or group of systems (router, proxy or gateway) designed to permit or deny network transmission based upon the set of security rules and regulations to enforce control between two networks to protect "inside" network from "outside" network. A firewall could also be a hardware device or a software program which might be running on a secured host computer [9]. Firewalls cease unauthorized access in the network from outside.
Basically, the fundamental rule is that all the traffic be it from inside or from outside must pass through the firewall. For doing this, all the access to the local network must first be physically blocked, and access should only be given via firewall. After that only Authorized traffic should be allowed to pass through a firewall. The important point here is that our firewall should also be strong enough to deal with such attacks.
In reference to Fig. 1 in [8] depicting "Organization of secure firewall based in E-learning systems" sophisticated firewalls can block some incoming traffic but allow E-learning users (admin, teachers, students, authors, systems developers, managers) inside to interact freely from outside interventions.
By this *Spoofing identity threat* and *Information Disclosure threat* of STRIDE model will be reduced.

ii). *Digital Right Management (DRM) on e-learning:* As we all know that E-learning systems are openly accessed systems. The biggest example of e-learning system is MOOCs – Massive Open Online Courses, where all the study material such as static HTML pages, or PDF document, or PowerPoint presentations, question papers, are shareable and freely available. Such freely available data as discussed above (in STRIDE model) can be accessed, changed, modified, copied and used very easily. Such a misuse of data could be reduced by DRM. DRM makes a system much safer to use for e-learning contents. DRM helps in digitization of data, by providing license agreement and copyright protection.

Hence, by this technique *Tampering of data threat* of STRIDE model will be reduced.

iii). *Cryptography:* the main purpose of putting so many restrictions is to maintain the confidentiality of user and data so that it is not misused by anyone. Different cryptographic tools and techniques could be used for implementing Security in internet based transactions. There are two major algorithms in cryptography namely- *Secret-key algorithms* and *Public-key algorithms* which includes; encryption decryption techniques, digital signatures, and digital certificates [9]. Hence, *Repudiation threat, Tampering of Data threat* and *Spoofing Identity threat* in STRIDE model could be reduced by this technique of cryptography.

iv). *Biometric Authentication:* out of all authentication techniques like passwords, usernames, pins, digital signatures, digital certificates etc. The safest is biometric authentication. The students can submit their assignments and papers through better security by biometric systems. The major drawback of this technique is- it is costly. Hence, *Information Disclosure threat* could be reduced by this technique.

v). *Digital Watermarking:* This technique allows to add hidden copywriter notices, audios, video, image signals so that multimedia database of E-learning system may be protected against unauthorized use [9]. The e-learning data like question papers, study material will be invisible to the intruder hence control over the system will also get difficult, hence resulting in less or no access to the system. Thus, *Elevation of Privilege* threat in STRIDE could be reduced by this technique.

IV. CONCLUSION

There is no doubt if we say that E-learning is the next future of learning. We are able to understand through this paper what E-learning system is, various E-threats, E-risks, E-remedies. People using the e-learning system for information learning should also get the little alert before sharing their personal data. The researchers, teachers, should keep a check on their data before it gets misuse. Administrators and Managers should keep should try to check the firewalls and Denial of service attacks. Still, there are many hidden threats which could not be detected or rectified yet. The Denial of Service attack in STRIDE model could not be reduced by any of the E-remedies techniques.

REFERENCES

[1]. Najwa Hayaati Mohd Alwi, Ip-Shing Fan, "E-Learning and Information Security Management", International Journal of Digital Society, Vol. 1, Issue 2, June 2010.

[2]. Zainal Fikri Zamzuri, Mazani Manaf, Adnan Ahmad, Yuzaimi Yunus, Book- "Chapter 30- Computer Security Threats Towards the E-Learning System Assets", Software

Engineering and Computer Systems, Publisher- Springer Berlin Heidelberg. Second International Conference, ICSECS 2011, Kuantan, Pahang, Malaysia, June 2011 Proceedings, Part II pp- 335-345, DOI-10.10007/978-3-642-22191-0_30, Print ISBN-978-3-642-22190-3, Online ISBN-978-3-642-22191-0.

[3]. I. Bandra, F. Ioras, K. Maher, "Cyber Security Concerns in E-Learning Education," International Conference of Education, Research and Innovation Seville, Spain. Proceedings of ICERI2014 Conference, ISBN: 978-84-617-2484-0, ISSN: 2340-1095, Published: IATED, pp. 0728-0734. Available online at: http://ecesm.net/sites/default/files/ICERI_ 2014.pdf.

[4]. Ankita Chopra, Aakanksha Chopra, "Application of Educational Data Mining Techniques in E-Learning Systems with its Security Issues: A Case Study", International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE),Vol.5 Issue 3, March 2016.

[5]. Zainal Fikri Zamzuria , Mazani Manaf, Yuzaimi Yunus , Adnan Ahmad" ,Student perception on security requirement of e-learning services", 6th International Conference on University Learning and Teaching (InCULT 2012), *Procedia-Social and Behavioral Sciences Journal,* Published by Elsevier ltd., 2013,Volume 90, 10 October 2013, pp 923-930. Available online at: www.sciencedirect.com.

[6]. Ateeq Ahmad, Mohammed Ahmed Elhossiny, "E-Learning and Security Threats", IJCSNS International Journal of Computer Science and Network Security, pp. 15-18, Vol. 12, No. 4, April 2012.

[7]. Zainal Fikri Zamzuria, Mazani Manaf, Adnan Ahmad, Yuzaimi Yunus, "Computer Security Threats Towards the E-Learning System Assets", Communications in Computers and Information Science, publisher Springer pp: 335-345, Vol-180 CCIS, ISSN (Print): 18650929, June 2011.

[8]. Nikhilesh Barik, Dr. Sunil Karforma, "Risks and Remedies in E-learning System," International Journal of Network Security & Its Applications (IJNSA), vol. 4, No. 1, pp. 51-59, Jan 2012, DOI: 10.5121/ijnsa.2012.4105. Available online at: http://arxiv.org/ftp/ arxiv/papers/1205/1205.2711.pdf

[9]. Aakanksha Chopra, "Security Issues of Firewall", International Journal of P2P Network Trends and Technology (IJPTT), pp. 4-9, Volume 22, Number 1, January 2016, ISSN: 2249-2615, Available online at: http://www.ijettjournal.org

[10]. The STRIDE Threat Model: by https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

[11]. Ahmad Tasnim Siddiqui , Dr. Mehedi Masud," An E-learning System for Quality Education ",IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 1, July 2012 ISSN (Online): 1694-0814

[12]. http://www.talentlms.com/elearning/what-is-elearning

[13]. Jennifer Olson, Kurt deMaagd, Joseph Codde, "An Analysis of e-Learning Impacts & Best Practices in Developing Countries With Reference to Secondary School Education in Tanzania", Information & Communication Technology for Development, pp: 1-53.