International Journal of
Science and Engineering Investigations vol. 8, issue 87, April 2019
Received on April 8, 2019 ISSN: 2251-8843

Cybersecurity Issues in Online Learning

Pee Vululleh
PhD., Professor, Missional University and Regent University, USA
(nohson16@yahoo.com)

Abstract-Cybersecurity is referred to as a set of techniques for ensuring the integrity, confidentiality, and availability of information. The core challenge of cybersecurity is to protect computer systems from unauthorized access. Online learning, which is a form of learning that occurs via the Internet, has evolved over the past decades as an area of concern regarding cybersecurity. While many educational institutions today are implementing online learning, the security of such systems presents unique challenges. Unlike face-to-face methods of teaching which depends on physical structures to house them, online learning is conducted via the Internet and accessed by unlimited numbers of users. With online learning, education can be facilitated from virtually anywhere and at any time conveniently and affordably by virtue of the technology. This paper presents a review of the most vital digital security challenges present within the higher education environment and it presents a security model for managing cybersecurity threats in the online learning context.

Keywords- *Cybersecurity, Cyberattack, Online Learning*

I. Introduction

Advances in technology have altered our lives and transformed the way in which we learn as students. Because of its demonstrated efficiencies, technology has the potential to play a major role in transforming the delivery of instruction in educational contexts. Online learning makes extensive use of interactive education technologies and participation by students in live lectures, video conferencing, interactive small group learning, and one-on-one tutorial (Czerkawski, 2016); further, such instruction can be delivered and received at any time subject only to the availability of Internet access for participants.

Unfortunately, the popularity of the Internet has created vast opportunity for cybercrime, such including property crimes, identity theft, and fraud. Because online learning fundamentally uses the Internet, information generated in this context, notably personal or confidential information is exposed to security threats. In response to increasing cyber threats, researchers have developed several countermeasures and solutions for improving security in online learning (García-Holgado & García-Peñalvo, 2016). Due to the broad variability within online learning systems, a 'one style fits all' approach would not fit all contexts and provide security against all cyber threats.

Given threat variability, this paper presents an approach to understanding and managing cybersecurity in online learning, starting with a review of the security challenges that are most important in current and future online learning higher education frameworks.

II. Cybersecurity and Education

Because of its demonstrated efficiencies, cyber technology has the potential to play a major role in transforming the delivery of instruction in educational contexts. Businesses and researchers show significant levels of interest in understanding how technology helps to create competitive edge for higher education institutions (Anderson, 2016; Erevelles et al., 2016; Mao et al., 2016). When technology is used properly, it facilitates better teaching and learning processes for both students and teachers. Unlike face-to-face methods of teaching, which depend on physical structures for a habitat, online learning provides a potentially superior alternative to face-to-face learning as it renders the "bricks and mortar" of educational institutions theoretically superfluous. With online learning, education can be propagated and received from virtually anywhere and at any time because of the convenience and affordability allowed by modern versions of technology.

In an online learning environment, encouraging engagement and trust building are paramount, since both synchronous and asynchronous communications are involved. Synchronous learning involves instructional interaction in real time (Moallem, 2015; Brierton et al., 2016; Rockinson-Szapkiw et al., 2016), where virtual classrooms allow users' comments to each other and to faculty to be instantly relayed; learners ask and instructors (sometime enabled by *artificial intelligence* routines) answer questions instantly. Online conferences and chat rooms are two examples of synchronous learning. In an asynchronous learning setting, communication is shared outside the constraints of a 24-hour clock (Moallem, 2015; Brierton et al., 2016; Rockinson-Szapkiw et al., 2016), learning can be accomplished even as learners are offline. Email and discussion forums are two examples of how asynchronous information sharing occurs in online learning.

Learning relies on the quality of relationships of trust and mutual engagement that users develop with and among each other. Studies have acknowledged trust to be a key enabler for knowledge sharing in online learning (Kuo, 2013; Ismail & Hosseini, 2014).

Trust is having confidence in others with the expectation that they will not disappoint one's expectations (Sicari et al. 2015). In an online learning environment, users build trust through familiarity and consistent, positive experiences (i.e., like getting to know others in the classroom).

III. Learning Management Systems Security

Learning management systems (LMSs) are the main component of online learning. LMSs are connected to the Internet and are thereby exposed to various threats. A review of literature shows that today's LMSs that support online learning do not adequately meet important security requirements (Hilmi et al., 2011). These systems normally provide collaborative learning experiences in their design but largely ignore security issues (Hilmi et al., 2011). This limitation may lead to unwanted circumstances that significantly affect online learning processes, such as network penetration, eavesdropping, unauthorized modification of data, hackers gaining access to students' information, non-availability of personal computers or servers, and student falsification of course assessments.

Public key infrastructures (PKIs) are essential to eliminating the cyber threats posed to online learning systems. PKIs ensure confidentiality, integrity, and authentication (CIA) in organizations that are required to minimize personally identifiable information exposure and manage the threat of risk (Misra et al., 2016). In an online environment, traditional password authentication, network perimeter security protections, and access controls often prove inadequate. Data traveling over the Internet must be protected by highly dependable encryption methods like the PKIs.

A. Cybersecurity Threats in Higher Education

Higher educational institutions are often targets for cyberattacks because of the vast amount of sensitive data they transmit and manage. For example, in 2018, the United States government charged nine Iranian hackers of orchestrating campaign to access and steal millions of records of sensitive information from over 300 American and foreign universities. In 2015, the Harvard University system was breached, although it remains unclear what information may have been accessed by the hackers. Similarly, in 2015, Penn State announced that their computer system was breached, with one of the attacks dating as far back in 2012, which comprised theft of the personal information of over 18,000 users. Among the biggest cyber issues facing higher education institutions is the intensity and persistence of cyberattacks that aim to steal personally identifiable information (PII), disrupt schools' ability to operate, and badly damage their reputations.

B. Social Media Sneaks

Today, cyber hackers infiltrate computer systems and install a piece of malware that can provide them control of the entire system and allow them to extract data. Social media and the openness of the Internet has thus become a major problem for higher education institutions. Hackers commonly gather intelligence about a university students, faculty, and employees and use this information to break into its computer systems. With state-sponsored cyberattacks, these processes occur over longer period, so they deploy a staff that spends a lot of time performing reconnaissance on different universities. Higher education's institutions are not aware of the most sophisticated methods that these hackers use to gather information. For example, they identify a university's IT staff with a LinkedIn profile that lists their positions, job responsibilities, and the software and hardware at which they are proficient. This information gives cyber hackers valuable tips about an institution's network systems. Higher education institutions need IT professionals with sophisticated cyber forensic skills to identify any unusual change to their systems.

C. Spear Phishing Threat

Spear phishing refers to an email spoofing attack that targets an institution or its employees to gain unauthorized access to sensitive data (Parmar, 2012; Gupta et al., 2017). The introduction and use of social media have helped spear phishing grow into a deceptive weapon with advanced sophistication. With spear phishing, hackers research an individual by name, place of work, residence, friends' lists on social media sites like Facebook and LinkedIn. With this information, they craft a communication which includes links or an attachment for download that looks appears legitimate for that user's consumption. Once the recipient clicks the link or downloads the attachment, their computer system is immediately compromised. These download attachments introduce malware into the recipient's computer system, which in turn helps the hackers steal passwords that can provide them access to the institution network.

When the IT department first becomes aware of spear phishing communication, they should immediately notify the entire university through social media, university official email accounts, or by any other means available. Employees who fall prey to spear phishing attacks should immediately notify the IT department, which will then provide suggestions and block the infected account or computer.

D. Smartphone Risk

Students, faculty, and employees use a variety of devices to connect to campus network systems. These devices are another easy target for cyber hackers because they are not secure compared to the institution's systems. With its lesser computing power and the user's inability to install security software because of the device's limited memory, cell phones (smart phones) are the worst security risk. Moreover, the software hackers' cost to hack phones and steal passwords and other PII is very low (Burkart & McCourt, 2017). Physical theft is also a major risk. If any member of a university system loses a phone for any reason, the phone can end in the hands of a hacker and provide that hacker with a means of entry in to institution's computer systems.

IV. Security Threats and Protection in Online Learning Systems

According to Alwi and Fan (2010), the accessibility of the system via Internet, users' consumption of the service via Internet, and payment of a service by the user are the three main characteristics of online learning systems. Therefore, management security approaches to protect against security threats in online learning are the same as they are for other electronic services. Some of the security requirements are described below:

A. Authentication

This process identifies the system's users and their access privileges. As such, authentication helps to prevent the cyber attackers from accessing legitimate users' accounts to view or steal sensitive information, which could then be used to perform unauthorized operations. Best practices regarding authentication include (a) obligating users re-authenticate their credentials at specified intervals, (b) requiring and enforcing strong passwords, (c) biometric-based security that cannot be duplicated easily or stolen, and (d) measures to prevent credentials from being passed or stored in plain text (instead employing secure socket layer —an encrypted link between a browser and a web server).

B. Access Control

This technique is realized during the authentication process when users are granted necessary rights, such as access to or privileges involving the systems and its resources. Access control techniques perform authorization identification, authentication, access approval and accountability through login credentials including personal identification numbers (PIN), passwords, electronic or physical keys, and biometric scans.

C. Confidentiality

In an online learning system, confidentiality is required to ensure that resources including course materials, assignments, and quizzes are available to students, faculty, and administrators who possess rights of access—and only to those who possess such rights. In this case, the user role should be clearly defined and given privilege as per requirements.

D. Integrity

In an online learning environment, integrity is needed to ensure that sensitive data and resources are available on the system and can be modified by only authorized persons and can be accessed only by users. For example, when students register for a course, they should be able to view the course materials when available. Only the instructor or authorized person, such as a teaching assistant, should be able to modify the contents for the course materials. To counter integrity failures, authorization measures should be strong to keep unauthorized users from altering information. Protocols should be tamper-resistant across communication links.

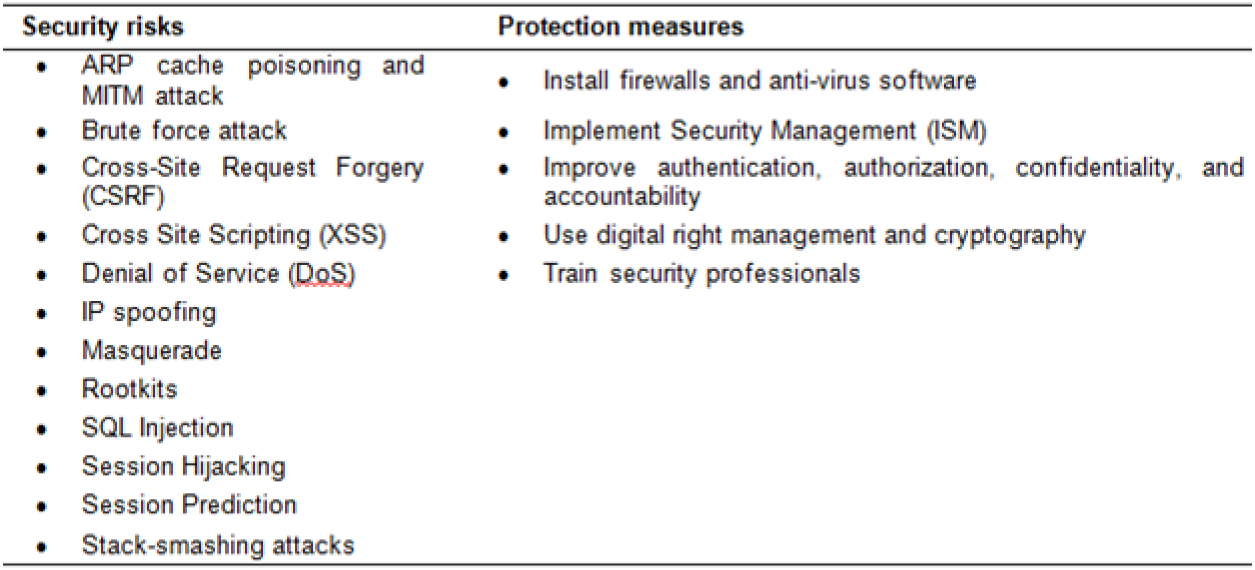
V. Online Learning Security Management Model

Online learning is mainly dependent on information and communication technologies. In an online learning environment, information may exist in many forms, such as written on paper or printed, electronically transmitted, or stored (Alwi & Fan, 2010). Whatever means are required to share such materials should always be protected to ensure the confidentiality, integrity, and availability of data. The following list recites the most serious threats to online learning system:

- *Denial of service (DoS)***:** Hackers attempt to make the systems unavailable to the legitimate users.
- *Viruses***:** Software when executed replicates itself through the modification of other computers programs and inserts its own code.
- *Human error or failure*: Employees make mistake or cause accidents.
- *Unauthorized access:* Persons illegally gain access into a computer system or network.
- *Vandalism or deliberate acts of sabotage:* Persons destroy systems or information.
- *Blackmail for information disclosure***:** Persons coerce or threaten to reveal true or false confidential information.
- *Hardware errors or failures***:** hardware errors that cannot be corrected by hardware.
- *Technological obsolescence:* outdated software or hardware.

A review of literature provides descriptions of protection for confidentiality and user authentication in online learning systems (Figure 1).

Technological advances have provided educational institutions with the ability to provide education to students in various ways, including the use of online methods. Such advances have also provided higher education institutions with the ability to detect and respond to data breaches instantly. Educational organizations create security management programs so they can implement effective controls. Effective online learning systems security depends on creating an environment and organizational structure where management understands and supports security efforts and encourages the users to exercise caution (Yuryna et al., 2017). Security teams should ensure that teachers, staff, students, and administration are aware of their security and support roles and are willing to accept the obligations, no doubt somewhat time consuming, that come with change and improvement. Figure 2 presents the process model developed for managing cybersecurity threats in higher education online learning system.



Security risks	Protection measures
• ARP cache poisoning and MITM attack	• Install firewalls and anti-virus software
• Brute force attack	• Implement Security Management (ISM)
• Cross-Site Request Forgery (CSRF)	• Improve authentication, authorization, confidentiality, and accountability
• Cross Site Scripting (XSS)	• Use digital right management and cryptography
• Denial of Service (DoS)	• Train security professionals
• IP spoofing	
• Masquerade	
• Rootkits	
• SQL Injection	
• Session Hijacking	
• Session Prediction	
• Stack-smashing attacks	

Figure 1. Online Learning Security Risks and Protections mechanisms

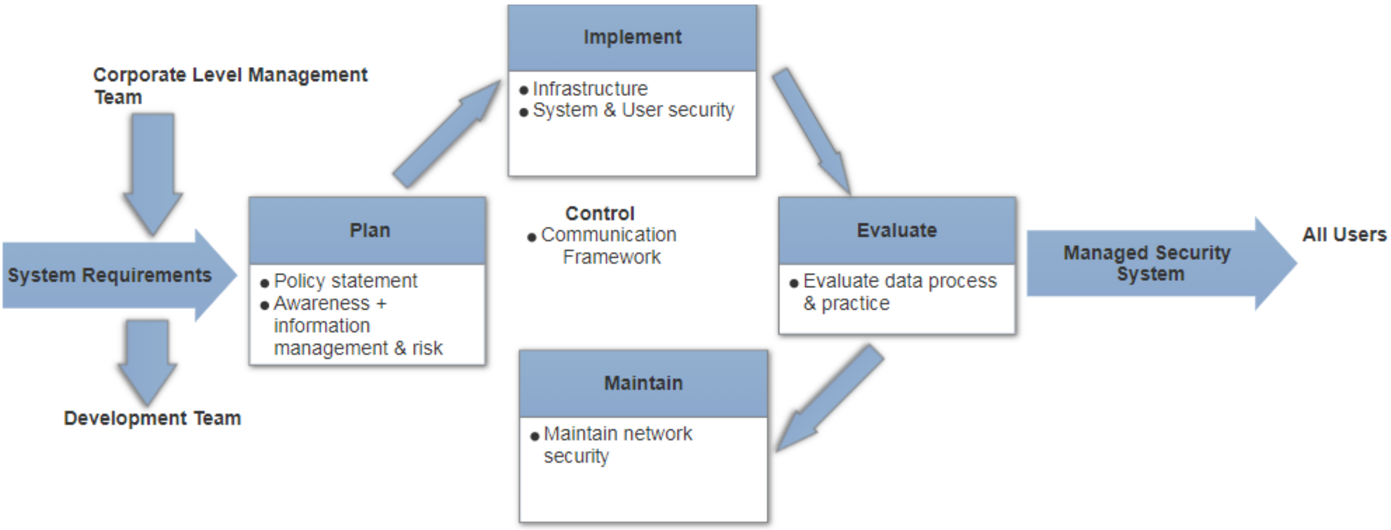


Figure 2. Cybersecurity threats process model in online learning (Adopted from Bandara et al., 2014).

Higher education institutions possess massive amounts of data about students, faculty, donors, staff, research programs, governmental information, and all manner of confidential material, making them tempting targets for cyber hackers. The risk of cyberattack increases with the emphasis on collegiality and openness that universities and colleges cultivate, demanding that institutions develop and enforce strategies to protect important data. Facing cyber security challenges not only involves software and hardware, but also an information security staff and strategies designed to educate users on how to protect networks and sensitive data both on and off campus.

VI. Conclusion

Online learning systems present a unique challenge to higher education because of their inherently cybersecurity challenges. This paper reviews the most vital security challenges that confront today's online learning higher education environments. Today, technology and education are firmly intertwined. The promised benefits of this synergy may be endless, but its survival depends upon successful response to criminal onslaught.

REFERENCES

[1] Alwi, N., & Fan, I. (2010). E-learning and information security management. *International Journal of Digital Society, 1*(2), 148-156. Retrieved from http://infonomics-society.org/wp-content/uploads/ijds/published-papers/volume-1-2010/E-Learning-and-Information-Security-Management.pdf

[2] Anderson, T. (2016). Theories for learning with emerging technologies. *Emergence and innovation in digital learning: Foundations and applications*, 35-50. Retrieved from http://www.veletsianos.com/2016/07/06/theories-for-learning-with-emerging-technologies/

[3] Bandara, I., Ioras, F., & Maher, K. (2014). Cyber security concerns in e-learning education. In *Proceedings of ICERI2014 Conference, 17th-19th November*. Retrieved from https://pdfs.semanticscholar.org/1bb6/b3165bae78910ca37bb350d534c70c31a7bb.pdf

[4] Brierton, S., Wilson, E., Kistler, M., Flowers, J., & Jones, D. (2016). A comparison of higher order thinking skills demonstrated in synchronous and asynchronous online college discussion posts. *NACTA Journal, 60*(1), 14. Retrieved from https://www.nactateachers.org/attachments/article/2377/7%20%20Brierton_NACTA%20Journal.pdf

[5] Burkart, P., & McCourt, T. (2017). The international political economy of the hack: A closer look at markets for cybersecurity software. *Popular Communication, 15*(1), 37-54. doi:https://doi.org/10.1080/15405702.2016.1269910

[6] Czerkawski, B. (2016). Blending formal and informal learning networks for online learning. *The international review of research in open and distributed learning, 17*(3). doi:http://dx.doi.org/10.19173/irrodl.v17i3.2344

[7] Erevelles, S., Fukawa, N., & Swayne, L. (2016). Big Data consumer analytics and the transformation of marketing. *Journal of Business Research, 69*(2), 897-904. Retrieved from https://EconPapers.repec.org/RePEc:eee:jbrese:v:69:y:2016:i:2:p:897-904

[8] García-Holgado, A., & García-Peñalvo, F. (2016). Architectural pattern to improve the definition and implementation of eLearning ecosystems. *Science of Computer Programming, 129*, 20-34. doi:10.1016/j.scico.2016.03.010

[9] Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications, 28*(12), 3629-3654. doi:10.1007/s00521-016-2275-y

[10] Hilmi, M., Pawanchik, S., & Mustapha, Y. (2011). Exploring security perception of learning management system (LMS) portal. *2011 3rd International Congress on Engineering Education: Rethinking Engineering Education, The Way Forward, ICEED*, 132-136. Retrieved from https://www.tib.eu/en/search/id/TIBKAT%3A793917883/

[11] Ismail, W., & Hosseini, S. (2014). Understanding online knowledge sharing intention: A factor analysis in E-Learning system. *Journal of Emerging Trends in Computing and Information Sciences, 5*(1), 9-20. Retrieved from http://www.cisjournal.org/journalofcomputing/archive/vol5no1/vol5no1_2.pdf

[12] Kuo, T. (2013). How expected benefit and trust influence knowledge sharing. *Industrial Management & Data Systems, 113*(4), 506-522. doi:https://doi.org/10.1108/02635571311322766

[13] Mao, H., Liu, S., Zhang, J., & Deng, Z. (2016). Information technology resource, knowledge management capability, and competitive advantage: the moderating role of resource commitment. *International Journal of Information Management, 36*(6), 1062-1074. doi:https://doi.org/10.1016/j.ijinfomgt.2016.07.001

[14] Misra, S., Goswami, S., Taneja, C., & Mukherjee, A. (2016). Design and implementation analysis of a public key infrastructure-enabled security framework for ZigBee sensor networks. *International Journal of Communication Systems, 29*(13), 1992-2014. doi:https://doi.org/10.1002/dac.2893

[15] Moallem, M. (2015). The impact of synchronous and asynchronous communication tools on learner self-regulation, social presence, immediacy, intimacy and satisfaction in collaborative online learning. *The Online Journal of Distance Education and e-Learning, 3*(3), 55. Retrieved from http://tojdel.net/journals/tojdel/articles/v03i03/v03i03-08.pdf

[16] Parmar, B. (2012). Protecting against spear-phishing. *Computer Fraud & Security, 2012*(1), 8-11. Retrieved from http://dev.faronics.com/assets/Spearphishing_BP_EMEA.pdf

[17] Rjaibi, N., Rabai, L., Aissa, A., & Louadi , M. (2012). Cyber security measurement in depth for e-learning systems. *International Journal of Advanced Research in Computer Science and Software Engineering, 2*(11), 107-120. Retrieved from http://www.ijarcsse.com, ISSN (Online): 2277 128X, ISSN (Print): 2277 6451

[18] Rockinson-Szapkiw, A., Wendt, J., Whighting, M., & Nisbet, D. (2016). The predictive relationship among the community of inquiry framework, perceived learning and online, and graduate students' course grades in online synchronous and asynchronous courses. *The International Review of Research in Open and Distributed Learning, 17*(3). doi: http://dx.doi.org/10.19173/irrodl.v17i3.2203

[19] Sicari, S., Rizzardi, A., Grieco, L., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer networks, 76*, 146-164. Retrieved from https://pdfs.semanticscholar.org/92ea/dd2ccae08b62ce4bccbd87ba46899accda2d.pdf

[20] Yuryna-Connolly, L., Lang, M., Gathegi, J., & Tyga, D. (2017). Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study. *Information & Computer Security, 52*(2), 118-136. doi: https://doi.org/10.1108/ICS-03-2017-0013

[21] Zare, H., Azadi, M., & Olsen, P. (2018). Techniques for Detecting and Preventing Denial of Service Attacks (a Systematic Review Approach). *In Information Technology-New Generations*, 151-157. Retrieved from https://link.springer.com/chapter/10.1007/978-3-319-54978-1_21

Dr. Vululleh works as a Professor at Missional University, and as Faculty at Regent University. He also serves on the Editorial Review Board for "The Journal of Business, Technology, and Leadership".

How to Cite this Article:

Vululleh, P. (2019) Cybersecurity Issues in Online Learning. International Journal of Science and Engineering Investigations (IJSEI), 8(87), 96-100. http://www.ijsei.com/papers/ijsei-88719-14.pdf