World Journal of Education and Humanities
ISSN 2687-6760 (Print) ISSN 2687-6779 (Online)
Vol. 3, No. 2, 2021
www.scholink.org/ojs/index.php/wjeh

Original Paper

Impacts of COVID-19 on Educational Institutions and their Instructional Approaches

Bishal Neupane[1] & Davar Pishva[1*]

[1] College of Asia Pacific Studies, Ritsumeikan Asia Pacific University, Beppu, Japan

[*] Davar Pishva, dpishva@apu.ac.jp

Received: February 22, 2021 Accepted: March 1, 2021 Online Published: March 3, 2021
doi:10.22158/wjeh.v3n2p1 URL: http://dx.doi.org/10.22158/wjeh.v3n2p1

Abstract

This paper examines various impacts of COVID-19 on Educational Institutions and demonstrates the results of their counter measures. In particular, it focuses on their online educational counter measure strategies and critically analyzes the system in terms of their numerous advantages, disadvantages and information security loopholes. It considers the advent of COVID-19 as a trigger for the improvement of educational approaches and foresees the continuous role of online education even after COVID-19. It demonstrates how a natural blend of online and traditional educational approach can improve both educational quality, its user oriented flexibility as well as reduce the adverse impacts of limited resources. While showing its conveniences, various economic and educational benefits, it also examines associated numerous security risks. It identifies security loopholes of online education as the main obstacle for its successful continuous adoption and provides necessary guidelines for its counter measures at various levels.

Keywords

Zoom, Cisco, e-learning tools, Confidentiality, Integrity, Availability

1. Introduction

In our modern era of Internet, mobile and digital information technology; adoption of innovative educational strategies to the needs of the time is quite important. This can be particularly true to private educational institutions whose main source of income is students' tuition fee. Higher education is considered as one of the most competitive industries in the United States, something which can also be true in many other countries. Higher education is now in a period of extraordinary change, driven by technology, globalization, changing finances and students' perspectives. While students are born and raised in this era, many educators are still straggling to efficiently adopt to the modern era. Being conscious of our competitive and dynamic environment and taking appropriate measures can be considered as key strategies towards success.

Since the expansion of the Internet in 1990s, digital information has become a social infrastructure for mankind. The technology has also penetrated to the field of education since it overcomes distance barrier between students and educational institutions. Its low overhead and numerous conveniences has led to its rapid expansion during the past three decades. The advent of COVID-19 and its rapid universal spread has raised its popularity to the highest ever seen peak. With the blessing of the Internet and online learning tools, students are able to continue their educational activities virtually while protecting their health as well as preventing their possible role in the spread of COVID-19. Such popularity and its associated huge network, however, has also created a new platform for hackers and attackers.

Online education is “flexible instructional delivery system that encompasses any kind of learning that takes place via the internet” (Jones, 2020). It is a virtual learning system that provides the whole educational materials through the internet. This way, educators can reach students at anywhere in any time, which might be much beneficial for those students who are not able to attend the traditional classrooms. On top of that, the flexibleness of online education would let them study on their own schedules and time, which is no less helpful than studying at the classrooms.

This work will descriptively analyze numerous benefits, challenges and security threats of online educational system and provide pertinent guidelines for its security counter measures. Section 2 gives a brief historical perspectives and transformation processes of online education. Section 3 critically analyzes online educational system from various perspectives; while showing its conveniences, various economic and educational benefits, it also examines associated numerous security risks. Section 4 focuses on its security challenges and provides necessary guidelines for its counter measures at various levels. Section 5 states its summary conclusions and provides some guidelines for future work in the field.

2. Historical Perspectives and Transformation Processes

The idea of online education system is evolved from the concept of distance learning. The concept of distance learning is said to be 170 years old, which was originated in Great Britain. At that time, the instructors would send the lessons to students and get assignments done by students by mail. Back then, distance learning did not include interaction, students-to-students communication; it was limited to only instructor-to-student communication and vice versa.

Internet based learning which was initially introduced by the University of Illinois started in 1960. The platform was called intranet at the time, which was a system of linked computer terminals where students could access course materials as well as listen to recorded lecture (PETERSON’S, 2020). Later, it evolved into PLATO (Programmed Logic for Automatic Teaching Operation) that could hold up to 1000 simultaneous users with the speed of 1200 bits per second (Jones, 2020). People could use it for messaging, chatting, reading articles and even playing educational games. Until this date, it took a long time for people to reach the era of computers and internet. Now, the life of a learners has become much easier, as most of the people have access to computers and the internet. In addition, getting those things in hand means getting full access to educational materials available throughout the internet. Furthermore, it has enabled people to study and interact with instructors and even with other students in real time.

2.1 Rapid Expansion of Online Education

There are many popular institutions that have provided online education during the past few decades successfully. Universities such as University of Florida, University of Illinois at Springfield, Texas Tech University, etc., provide online education to those students who cannot be in the campus physically (Best Colleges, 2020). The quality of online education is equally maintained in these institutions to match that of on-campus education system. Since there are no educational materials which cannot be accessed from home/or from anywhere, quality of their online graduates are similar to those of on-campus graduates. These universities offer students the choice of online and on-campus education. In addition to that, students can apply for scholarships regardless of their selected educational approach. Such kinds of incentives and offers could encourage students who want to learn online and help online learning systems to gain popularity.

Online education can also play an important role when there are significant shortage of experts in a particular area. For example, the year that the “Personal Information Protection Act” (“PIPA”) came into effect in Japan in 2005, Hyogo Prefecture decided to play a leading role in addressing the issues of the much-needed cyber security and information and privacy protection. Sensing a significant shortage of experts in information security and an urgent need to train competent leaders, it joined hands with Carnegie Mellon University, a world leader in the area of information security, established CyLab Japan, and by relying on the state-of the-art remote lecturing technology, brought top-quality security education to Japan in an amazingly short period of time (Pishva, 2007). The program enabled Japanese students to acquire world-class security education and obtain US degrees without leaving Japan.

2.2 Role of Learning Management System on Online Education

Although online education can be acquired from anywhere through the internet, learning management system (LMS) plays a significant role in its process. LMS is a software application or web-based technology that can be used to plan, implement and assess a specific learning process. It provides instructors with a way to create and deliver content, monitor student participation and assess student performance (Rouse, 2020). LMS can serve as an effective and speedy approach to gather information.

There are many types of LMSes and each one is designed for specific purposes. Some of the popular ones are as follows:

a) Cloud-based LMS:

This type can be accessed from anywhere at any time as it is hosted on the cloud. It requires only user ID and password to access the system. Its system maintenance and upgrade are done by the administrators.

b) Self-hosted LMS:

This type requires users to download the software as well as input User ID and password for its access. Users are also responsible for its maintenance and upgrades. Nonetheless, such type allows users to customize the system to their specific operating procedures.

c) Desktop application LMS:

There are some LMSes which can only be installed on desktops. It may not allow download from multiple devices, which can create difficulties to access the system from different places.

d) Mobile application LMS:

Such type can be very convenient as it can be accessed from anywhere at any time. However, considering smaller screens of smart phones, its readability may not be as clear as desktop ones.

2.3 Impacts of the Covid-19 on Online Education

Online education and virtual classes was an alternative for students until the Corona Virus breakout in 2019. However, it has become necessity of every student in the world during this pandemic, as no one would risk their lives to go and study in traditional classrooms. Schools and other educational institutions were shut down completely during the starting phase of the COVID-19 breakdown and students had to stay at home doing nothing due to that. Figure 1 shows the number of students whose educational activities were adversely affected during the early stage of COVID-19.

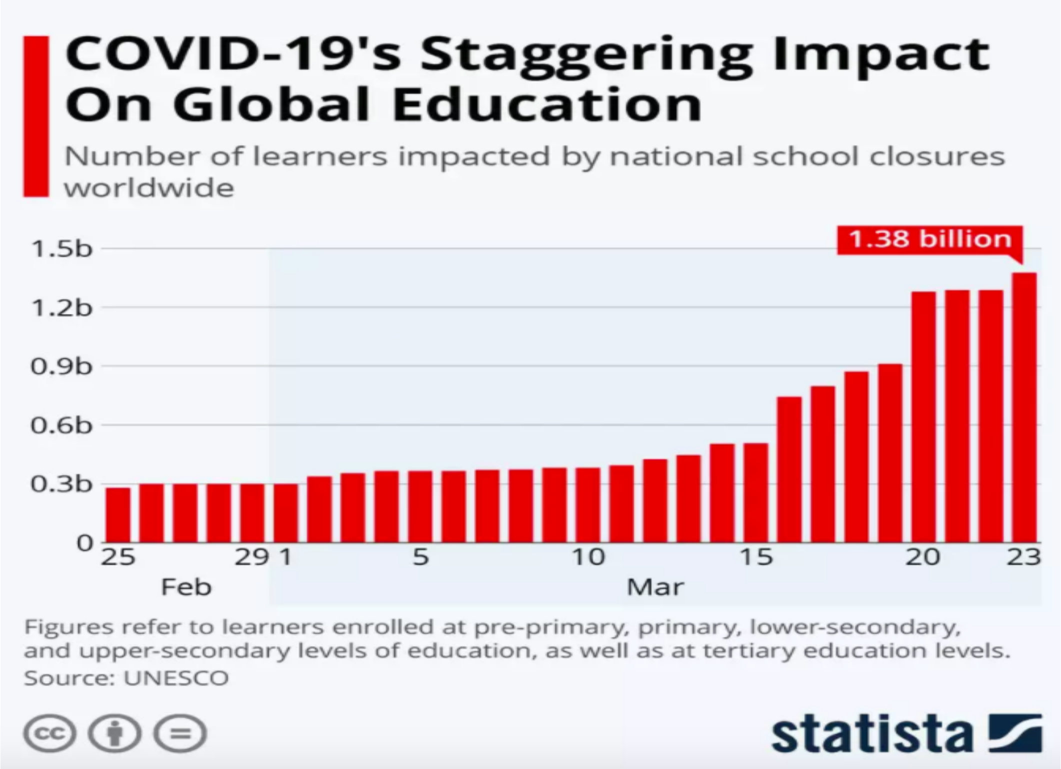

Figure 1. Number of Students Whose Education Was Affected during the Early Stage of COVID-19

Source: https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning/

During that state of emergency, the online education system became a temporary solution for resuming schools and classes. In the present situation, COVID-19 has not shown any sign of retreating which has led the world to stick into the online education for now. Thus, there is a good chance that E-learning system would influence the way of education permanently. May be traditional classes will never be the same as before. Rather, it might get transformed into an integrated version of online and traditional way of education so as to improve educational quality and its user oriented flexibility.

People have learned that online education is not only about distance learning but also it gives access to lots of study materials to students. Therefore, instructors would use this combined approach to teach the students and guide them to learn and understand better. This would increase the number of online authors, learning management systems, and online education business and eventually lead the competition among them. The market competition may actually help learners to gain access to more materials for free. Although COVID-19 is a nightmare for humanity, it may trigger a change in the way of learning afterwards.

2.4 History of Cyber-Attacks on Online Education

The higher education sector increasingly attracts hackers due to huge amounts of critical information its system store. Such information include personal information of their employees and students as well as their proprietary research materials. A research conducted by EdGuards Company, which describes cybercrime development in the U.S. Higher Education sphere and notorious incidents caused by malefactors' activity, reveals that a starting point of data breaches dates back to 2002 (Lynn, 2020).

– Attack on Yale's system in 2002 by hackers from Princeton University, targeted information on the admission decisions.

– In 2003, several attacks directed on students' and staff members' personal information

– About 2,000,000 records of California universities were stolen in 3 breaches in 2004

– In 2005, personal data of 150,000 students, staff and library of University of Hawaii were stolen by a former librarian.

– In the same year 2005, 100,000 names and social security numbers of former employees were stolen from University of Utah.

– In 2006, nearly 800,000 records of faculty and staff, parents and students' applications were lost due to the breach on University of California.

– In March 2018, over 300 universities worldwide suffered from a giant cyber-attack which was organized by nine Iranian hackers. According to the official information, 31 terabytes of "valuable intellectual property and data" were exposed. This case became one of the biggest hacker campaigns.

– During 2014-2016, not only the number of attacks rose significantly, but also breaches became more aggressive and advanced. The main point of this period was a considerable increase in number of attacks. According to the statistic provided by Verizon's annual Data Breach Investigations Report, the frequency of security breaches affecting universities multiplied almost ten times. By 2017, the number of cyber-attacks vastly grew to 393 while in 2012 there were only 5 (Lynn, 2020).

– Figure 2 shows the percentage of educational resources hit by distributed denial of service (DDOS) attack globally during the past two years. According to the source, DDOS attacks to the online learning system in 2020 have increased by 80% compared to 2019. The green bars in the figure represents percentage of the attacks in 2019, and the red bars represents those of 2020.

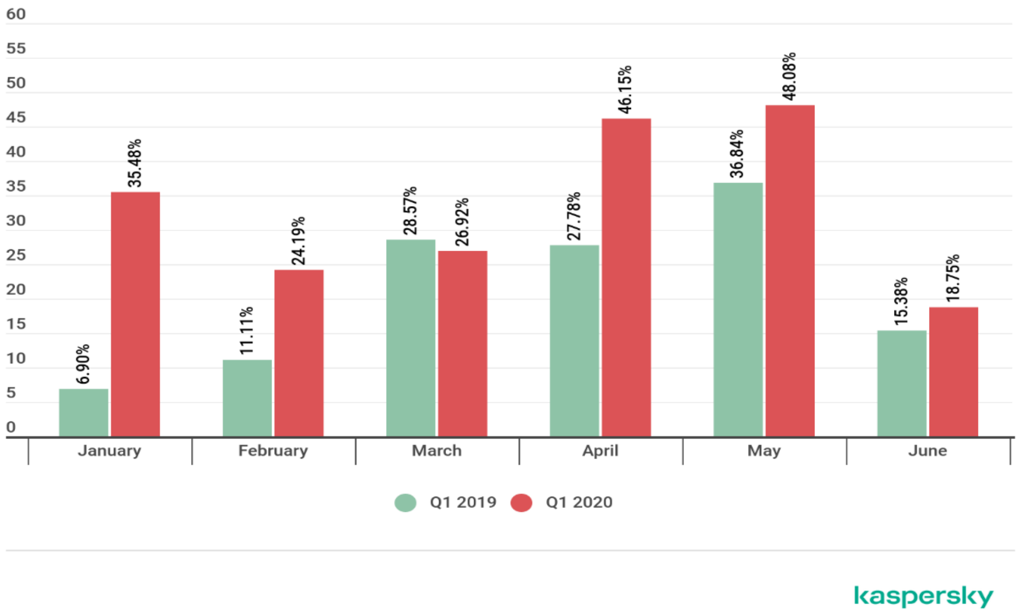

Figure 2. Percentage of Educational Resources Hit by DDOS Attacks during 2019-2020

Source: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2020/09/03105019/04-en-education-report.png

3. Conveniences and Challenges of Online Education

It cannot be said that online learning method is superior to the traditional one or vice-versa since both methods have pros and cons. In general, it depends upon individual's preference and institutional settings, something which can be influenced by many external and internal factors. Such factors can be economic, convenience, time saving, job, flexibility, and measures to cope up with resource limitation.

3.1 Conveniences of Online Education

Online education system certainly has a number of benefits that makes it popular these days. Features like flexibility and self-paced learning, time and money saving, etc., makes it more convenient and reliable for online learners. Aside from these, there are other benefits and conveniences of online education, summary of which are as follows:

– Variety of programs and courses: Similar to traditional schools and universities, online educational institutions are also able to offer variety of programs and courses to students. Students can choose their desired courses without any barrier and they shall be guided towards their academic degrees.

– Comfortable learning environment: Students attending virtual classes do not have to wear uniforms, or be careful of their sitting posture. They neither have to leave early for school nor miss an important family occasion. Many students find the online education comfortable because they do not need to worry about such things. Their main objective is to learn and it can be achieved through online education.

- More interaction and greater ability to concentrate: Online courses offer shy or more reticent students the opportunity to participate in class discussions more easily than face-to-face class sessions. Some students even report better concentration in online classes due to the lack of classroom activity (OEDb, 2020).
- Continuity in the profession: Online education can be a better option for those students who want to pursue their education while having a job. This way they can avoid commuting time, have a flexible schedule and continue their job and education at the same time if managed well.
- Eco-friendly: Considering that students do not need to commute to a college or university for pursuing their academic degree, can result in fuel combustion reduction and emission of harmful gases to the environment.
- Around the clock availability of course materials: Students can readily access online course materials such as videos, podcasts, written materials to reinforce course concepts and theory. This way, they can improve their understandings on ambiguous topics. (Dumbauld, 2020)
- Development of self-discipline: Considering lack of physical presence of professors in online learning system who set the rule and bound the students with discipline, students have to learn self-discipline to manage time and tasks. This can lead students to learn on their own and acquire a life-long skill that can help them beyond their university life. (Dumbauld, 2020)
- Widening the scope of limited resources: Considering the natural potential of online education for collaboration and networking, limited precious resources of educational institutions can be easily shared in a mutually beneficial manners. Rapid advancement of science and technology along with our competitive and dynamic environment make such collaborative approach essential for faster progress.

3.2 Challenges of Online Education

Online education can be beneficial and convenient to those students, who have started to learn remotely initially. However, it can be equally difficult and challenging for those students who are unprepared and forced to switch into online learning system from traditional learning due to the COVID-19 pandemic. Some students who are keen to learn face to face with teachers may not find the online learning effective and satisfying. Due to the pandemic, reputed colleges and universities that used to operate the classes traditionally might be facing many technical and time management issues. As for teachers and professors, they might have to cope with their existing syllabus and teaching styles. To conclude, switching to online learning from traditional learning system was never easy to any educational entities, neither students, nor educational sectors or professors. Still, these entities are trying to fix the errors and problems to carry out the online education effectively and efficiently. Yet the challenges that the students are facing comes first in a row. Some of the challenges are as follows (Friedman, 2020):

- Technical issues: This is the most common issue faced by many students during the process of online learning. Crashing of server, crashing of device, internet issues, etc. are usually faced while having video conferences and lectures. During the time interval of rebooting and restarting of the devices and the internet, which takes few minutes, users might lose significant portion of lectures.
- Distractions and time management: While studying, learners need quiet place to continue an effective learning process and the most suitable place to learn is no other place than colleges or universities. During online learning, mainly while having a virtual class in real time, students might experience distractions from family member, friends or from strangers if they are learning at public places. These distractions would slow down the pace of learning, and eventually it hampers the time management of the students.
- Staying motivated: To stay motivated in learning, most of the students need physical campus and presence of professors. Lack of such physical setup may affect students' motivation. Therefore, students may need to find a way to get motivated while learning at home or from private or public places. They should find a space where they can stay focused for an effective learning.
- Understanding course expectations: The sudden switch to online learning has left some students confused about some course requirements for the rest of the semester. They may wonder, for instance, if a final group presentation is still happening given that students can no longer meet on campus, or if they need to complete labs for science classes. Students may also wonder whether their classes will have live lecturers through videoconferencing at a set time on a certain day, or whether students are expected to learn the material on their own time (Friedman, 2020).
- Lack of in-person interaction: For those students who extensively enjoy learning in the physical environment, online learning can be very inconvenient and challenging. Most of the younger students who have recently started university education would find online learning dissatisfying. On the other hand, regardless of age group, subjects like chemistry, biology, etc. that requires self-practice are next to impossible to study remotely. This is one of the negative aspects of online learning system.
- Adapting to unfamiliar technology: Sudden switching of the paper-based learning system into the digital system is a huge change in education system. Users need to learn to adapt at first, but it is not a big deal to those people who had prior knowledge about digital or online learning. However, it can be very difficult to those who have no knowledge about the technology. Especially, students in developing and un-developed country who did not have access to computer and internet in the past, may need to learn about technology at first. The author has personally received complaints from some students regarding their inability to type during online exam sessions. The same thing can also be true for elderly professors and those who are hesitant to change their traditional approach.
- Uncertainty about the future: Due to the outbreak of COVID-19, almost all of the schools and campuses had to switch into the online learning system. Those students who were learning physically at schools had a panic about their academic future. Many of the students were not sure if the transition to online learning would help in their career building. Now, it seems most of them are satisfied with it.

4. Security Challenges of Online Education and Possible Solutions

E-learning system has become an ultimate solution for a smooth operation of educational activities worldwide during COVID-19 pandemic situation. The system has now been upgraded to a more advanced level than the past. However, considering that online education system is an internet based learning system, information security plays a vital role on its smooth operation. Unfortunately, its security level has not proportionately advanced. This is mainly due to the fact that it does not directly deal with money or other banking transaction.

As such, the higher education sector increasingly attracts hackers due to large amounts of critical information their systems store. Furthermore, huge network of online education, their security unaware users and somewhat relaxed security measures compared to financial institution, makes the platform an ideal place for hackers and attackers to experiment with their new hacking techniques.

4.1 Typical Security Attacks on Online Education

Although security attacks on online education does not happen on daily basis, it can happen several times per month. The most common types of attacks are as follows:

a) Distributed Denial of Service (DDOS) Attacks:

DDOS attack is one of the most powerful weapons in the internet which is used for crashing down a website with too much traffic. The aim of the attack is to crash down a specific website by flooding more traffic than its server or network can accommodate (Weisman, 2020). It is mostly performed by the hackers via a program (called under various names; e.g., bot, robot, zombie, drone) that secretly takes over hundreds or thousands of Internet-attached computers and Internet of Things (IOT). It then uses those computers/IOTs to launch simultaneous attacks that are difficult to trace to the bot's creator. The collection of bots is referred to as a botnet. In most cases, online learning websites are vulnerable to these attacks due to their weak security implementation as they do not deal with monetary issues. Furthermore, considering that most of their users are security unaware, their computers can also be transformed into bots and serve as a botnet. Hackers can therefore take advantage of these weaknesses and try to experiment with their new attacking scheme. Previously shown Figure 2 revealed an 80% increase in DDOS attacks on online learning systems in 2020 compared to those of 2019 attacks.

b) Phishing Risks:

Phishing is one of the oldest and most popular forms of cybercrime. It has now reached to online learning platforms and video conferencing applications. A host of phishing websites for popular platforms like Google Classroom and Zoom began to pop up following the switch to distance learning. From the end of April to mid-June of 2020, Check Point Research (Peters, 2020), discovered that 2,449 domains related to Zoom had been registered, 32 of which were malicious and 320 were "suspicious". Suspicious domains were also registered for Microsoft Teams and Google Meet. Users who land on these phishing pages are often tricked into clicking URLs that download malicious programs, or they might be tricked into inputting their login credentials, which would put these in the hands of the cybercriminals (Kaspersky, 2020).

c) Cross Site Scripting (XSS):

XSS is a common attack vector that injects malicious code into a vulnerable web application. XSS differs from other web attack vectors, in that it does not directly target the application itself. XSS in itself is a threat which is brought about by the internet security weakness of client-side scripting languages, with HTML and JavaScript as the prime culprits for this exploit. The concept of XSS is to manipulate client-side scripts of a web application to execute in the manner desired by the malicious user. Such manipulations can embed a script in a page which can be executed every time the page is loaded, or whenever an associated event is performed. An XSS attack can result to accessing sensitive information, identity theft, altering browser functionality, web application defacement, and denial of service attacks (Magdalena, 2012).

d) Cross-site Request Forgery (CSRF):

CSRF is an attack that tricks the victim into loading a page that contains a malicious request. It is malicious in the sense that it inherits the identity and privileges of the victim to perform an undesired function on the victim's behalf, like change the victim's e-mail address, home address, or password, or purchase something. For most sites, browsers will automatically include such requests with any credentials associated with the site, such as user's session cookie, basic authentication credentials, IP address, Windows domain credential, etc. Therefore, if the user is currently authenticated to the site, the site will have no way to distinguish this from a legitimate user request. This way, the attacker can make the victim perform actions that they did not intend to, such as logout, purchase item, change account information, retrieve account information or any other function provided by the vulnerable website (Magdalena, 2012). Since most of the applications and web sites of online learning platforms are vulnerable, they have high probability of facing these kinds of attacks.

e) SQL Injection:

This is a relatively simple type of attack through which a hacker can pass string input to an application with the hope of gaining authorized access to a database. Hackers enter SQL queries or characters into the web application to execute an unexpected action that can then act in a malicious way. Such queries can result in access to unauthorized data, bypassing of authentication or the shutdown of a database even if the database resides on the web server (Magdalena, 2012).

f) Session Hijacking:

Session hijacking is a method of taking over a web user session by secretly obtaining the session ID and masquerading as the authorized user. Once the user's session ID has been accessed, the attacker can masquerade as an authentic user and do anything the user is authorized to do on the network. The session ID is normally stored within a cookie or URL. Session hijacking takes advantage of that practice by intruding in real time, during a session (Rouse, 2020).

4.2 Possible Security Counter Measures

Considering the fact that most security software are equipped with security counter measures for most types of known attacks, properly equipped computers can block most types of such attacks. However, not all computers are equipped with such security software. Furthermore, low end computers, mobile devices and battery powered systems cannot handle long-lasting or high-peak computations which are required in computationally expensive cryptography. The issue of security counter measures can therefore be narrowed down to user equipment, security implementation policies and governance systems. On top of that, security awareness of the system users also play a crucial role in the process. No security will work when a user does not properly select/protect his/her passwords for various Internet services or does not know what Phishing is, clicks such links and provide the requested information. Systematic security counter measures of online education can therefore be achieved through the following three steps:

4.2.1 Immediate Necessary Safeguard Actions

Considering the advent of COVID-19 and its rapid universal spread, our globalization trends and increase in competition, immediate strict implementation of security scheme may be difficult. Nonetheless, educational institutions and online learning tool providers can highly recommend the following guidelines:

- Selection of strong password when creating an online learning account.
- Utilization of security software equipped computers when connecting to online sessions.
- Keeping their software up-to-date so as to protect them against the known attacks.
- Individual users should close unnecessary applications and avoid long idle time. Complete system shut down should be carried out when a foreseen idle time would exceed an hour.

4.2.2 Intermediate Schemes

Now that the Internet is an indispensable part of our social life, educational and business activities, security awareness and pertinent education for the common people is also quite important. Unfortunately, even in a highly industrialized country like Japan, information security awareness is not part of general education even at university level! Since COVID-19 and its rapid universal spread has raised popularity of online education to the highest ever seen peak, it should also be used as an opportunity to include an introductory course in information security as part of the required liberal art course at university level throughout the world. Educational institutions that do not possess local resources for such conduction, can rely on the magic of online education and retrieve lectures from partner institutions. This is mainly because in our era of Internet, an appropriate education, training, guidelines, policies and governance systems in information security are equally important. Let us not forget that no information security counter measure will work when their users are illiterate about it.

4.2.3 Long Term Security Strategy

A comprehensive long-term security implementation strategy should be taken from various perspectives and it would require governmental and institutional policies, their strict implementation by online learning tool providers, learning management system suppliers, digital information providers and their numerous users.

The fact that higher education is considered as one of the most competitive industries, their provided contents via online learning systems are considered as proprietary materials. Its proprietary nature can be institution specific as well as faculty specific. Hence, they should only be accessible to peoples to whom they are intended for.

Furthermore, it should also be noted that some attackers are neither interested in such proprietary materials nor in the personal information that these institutions store. Such groups consider the huge network of online education, their security unaware users and somewhat relaxed security measures, an ideal platform to both experiment with their new hacking techniques as well as transform their weak security clients into botnet for their intended other attacks.

The fact that such attacks adversely affects third parties rather than their online educational institutions, implies moral, social and "hopefully in the near future" legal obligation for less attentive parties. The same thing can apply to malicious use of proprietary materials. Hence, explicit governmental and institutional policies are required for both protecting proprietary nature of educational contents as well as prevention of becoming instrumental gadgets for third parties attacks.

5. Conclusions

This work showed how online education has expanded since the era of Internet and its highest ever reached peak level during the advent of COVID-19. On top of showing its absolute necessity during the COVID-19, it demonstrated how online education is going to permanently influence traditional education. It critically analyzed online educational system in terms of their numerous advantages, disadvantages and security loopholes. While showing its conveniences, numerous economic and educational benefits, it also examined its shortcomings as well as associated numerous security risks. It foresees COVID-19 as a trigger to transform the traditional education into a hybrid platform so as to improve educational quality, its user oriented flexibility as well as reducing the adverse impacts of limited resources. It considered security challenges of online education as the main obstacle and proposed appropriate counter measures. It highlighted the importance of security awareness of its users, pertinent governmental and institutional policies as well as responsibilities of its numerous stakeholders. For a successful adoption of innovative educational strategies to the needs of the time, proper handling of its associated security risks is quite important. Considering that the main role of educational institution is to provide education, it is essential to start educating their clients and numerous stakeholders on information security. Furthermore, now that the Internet is also an indispensable part of our social life and business activities, security awareness of general public is important too. Let us not forget that being conscious of our competitive and dynamic environment and taking appropriate measures is a strategic step towards success.

Further studies along this field can be done from various perspectives and this section mentions a few important ones.

– Considering the universal nature of our approach and proposed strategy, further studies can custom tailor them to a specific region, culture, and economic settings.

– The fact that this work started at the beginning of COVID-19 and got finalized at its early stage, its presented actual data has been limited to the available ones at the time. When enough data becomes available, a more scientific approach can be employed to model, simulate and predict future educational strategy at both regional and universal level.

– A survey on the feasibility of particular learning management systems, virtual educational tools and hybrid teaching strategies to specific countries or regions' settings from various perspectives can also be beneficial.

References

Best Colleges. (2020, 07). *Best Online Colleges & Top Online Universities of 2020 | BestColleges.com*.

Dumbauld, B. (2020, 10). *13 Benefits of Online Learning | Straighterline*. Retrieved from https://www.straighterline.com/blog/34-top-secret-benefits-of-studying-online/

Friedman, J. (2020, 10). *How to Overcome Challenges of Online Classes Due to Coronavirus | Best Colleges | US News*. Retrieved from https://www.usnews.com/education/best-colleges/articles/how-to-overcome-challenges-of-online-classes-due-to-coronavirus?rec-type=usn

Jones, C. L. (2020, 07). *Online Education | Encyclopedia.com*. Retrieved from https://www.encyclopedia.com/finance/finance-and-accounting-magazines/online-education

Jones, S. (2020, 07). *PLATO | computer-based education system | Britannica*. Retrieved from https://www.britannica.com/topic/PLATO-education-system

Kaspersky. (2020, 11 20). *Digital Education: The cyberrisks of the online classroom | Securelist*. Retrieved from https://securelist.com/digital-education-the-cyberrisks-of-the-online-classroom/98380/

Lynn, A. (2020, 11 12). *Cyber Attacks History In Higher Education | Information Security Buzz*. Retrieved from https://www.informationsecuritybuzz.com/articles/cyber-attacks-history-in-higher-education/

Magdalena, C. L. (2012). *Procedia Social and Behavioral Sciences*. E-learning Security Vulnerabilities, 2297-2301. Available on Proc. https://doi.org/10.1016/j.sbspro.2012.05.474

OEDb. (2020, 08). *10 Advantages of Taking Online Classes | OEDB.org*. Retrieved from https://oedb.org/ilibrarian/10-advantages-to-taking-online-classes/

Peters, J. (2020, 11 20). *Hackers are impersonating Zoom, Microsoft Teams, and Google Meet for phishing scams - The Verg*e. Retrieved from https://www.theverge.com/2020/5/12/21254921/hacker-domains-impersonating-zoom-microsoft-teams-google-meet-phishing-covid-19

PETERSON'S. (2020, 07). *The history of online education – Peterson's*. Retrieved from https://www.petersons.com/blog/the-history-of-online-education/

Pishva D. (2007) Smart Classrooms Bring Top-Quality Education Around the Globe. *IEEE International Symposium on Applications and the Internet (IEEE SAINT2007* (pp. 40-43). https://doi.org/10.1109/SAINT-W.2007.97

Rouse, M. (2020, 07 18). *What is a Learning Management System (LMS) and What is it Used For*? Retrieved from SearchCIO:https://searchcio.techtarget.com/definition/learning-management-system

Rouse, M. (2020, 11 20). *What is session hijacking (TCP session hijacking?)-Definition from WhatIs.com*. Retrieved from https://searchsoftwarequality.techtarget.com/definition/session-hijacking

Weisman, S. (2020, 11 20). *What Is a DDoS Attack? Distributed Denial-of-Service Attack Explained* | *Norton*. Retrieved from https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.htm

Hilts, P. J. (1999, February 16). *In forecasting their emotions, most people flunk out*. New York Times. Retrieved November 21, 2000, from http://www.nytimes.com