RISK ASSESSMENT

Information Management and Control

7114 IBA

Aakash Bhavsar (s5152710)
Ammad Rahil Rao (s5174087)
Gowtham Ravi (s5190712)
Rajat Bamb (s5151978)

Table of Contents

1. EXECUTIVE SUMMARY

Online learning has been drastically increasing over the past couple of years. Recently, due to the COVID-19 pandemic, many high schools have rushed into adopting online teaching. Given the circumstances, the schools and teachers lack skills in operating the online learning environment. Regardless of the situation, every school and university must be aware of the risks involved. Several such incidents and their consequences have been highlighted that show a bigger picture. Upon assessing the risks, the damage that can be done to the institution and individuals raise numerous amounts of concerns regarding well-being, finance, reputation, cyber threats, and much more. Lastly, some best practices, policies, legal and technical recommendations have been made to mitigate the risks and vulnerability.

2. INTRODUCTION

St. P's is a high school in a remote Indian region that does not have any form of internet technology to provide students with an educational environment. The school has decided to settle on the Google Meet as their technology of choice for delivering classes online because of COVID-19. Furthermore, as it is a school in a small town and no one knows how to use the online learning system, the lack of training and awareness is evident to the Head of the school and employees. Provided the circumstances, during the pandemic, the school eventually managed to commence the classes and provide the students with education.

The advantages of using online education being improved interaction such as platforms allow for the exchange of detailed information on projects and exams through video and audio messages and insights into student learning.

The risk assessment document focuses on St. Paul's high school, which has an improper risk control system and challenges in recognizing the use of preventive measures needed to manage the risks. The detailed reasoning of the due to which the school faced the security risks and presented the recommendations for the risks found in relation to the St. Pauls' high school.

3. RESEARCH

Risks associated with online learning that the school could be vulnerable to are highlighted below:

Every technology comes with some sort of risks, so does e-learning. Online learning solely depends on the internet, where many illegal activities and security threats are bound to happen. Therefore, there are constant risks, threats, and attacks which can lead to unauthorized modification and/or destruction of educational assets. According to Alwi and Fan, in 2010, many schools and institutions are rushing to adopt this tech without proper planning and analyzing the consequences of the threats. Identity theft, impersonation, and inadequate authentication are some of the major risks that must be considered in online teaching (Chen &

He, 2013). Hackers are increasing day-by-day, and educational institutions remain one of the easiest targets for them to retrieve various types of information. Thus, the added functionality and advanced features make it more exposed to security threats**.** Sometimes, some courses require additional support and the use of tools just as blogs, wikis, or docs that have their own mechanism to control as to what and how the information is to be shared, so the teachers have limited control over data sharing (Chen & He, 2013)**.** Some tools require the installation of special software or plug-ins such as Endnote, but it is difficult for instructors to make sure the right plug-in is downloaded, and there's no spyware in the software (Singh**,** Mangalaraj and Taneja, 2010).

Tools like learning management systems are accountable for exploitation, which have disastrous effects on the accessibility, availability, and reliability of the platform. This may affect the day-to-day activities of the educational institutions and their long-term reputation. Australian researchers discovered that Blackboard Learn, a platform used by several universities throughout the world, had several zero-day vulnerabilities that led students to change their grades and download the future assignments, exams, and several other relevant information (Schultz, 2012). Research proves that internal threats are possible in any information system and highlights a similar incidence. In 2008, the University of Texas Brownville's staff and student worker used admin credentials to access the university's Blackboard system to steals exams. Another similar incident at Baylor University shows that a breach by a student costed the personal data of over 500 students, staff, and faculty (Daily, 2008) as cited in (Schultz, 2012).

According to the study, there are two aspects of security threat -user side and management side. Lately, the use of social media apps, along with a learning management system, is increasing drastically. Teachers find it convenient to share some of the stuff via social media apps. However, a report by a leading security company, Kaspersky (2009), reported that apps or sites used by students have a good atmosphere for hacking, deception, abuse, and misuse. Personal data posted on such sites can be used for virtual insult or cyberbullying or even worse financial gain. Malware is more likely to be delivered on such sites by phishing (Patel et al, 2012) as (Wang & Heffernan, 2010). Instructors and teachers have to collect some personal information from students like phone number, birthday, birthplace, age, facial photo, or even address. They have uploaded homework, online collaborative projects, and the grades of assignments as the personal information of the students, which can be easily leaked and spread when stored electronically. Most of the new teachers lack proper training and sometimes is very prominent (Kearns et al., 2014). Moreover, teachers develop their skills, mostly by observation and experience. Even a single course can lead to many digital copies so, and teachers find it quite challenging to manage thousands of digital artifacts effectively and efficiently (Wang & Heffernan, 2010).

Information loaded on the websites by many users simultaneously may cause congestion. This may lead to unanticipated costs in terms of both time and money (Collins et al, 1997) (Arkorful & Abaidoo, 2015). Another serious threat to information in e-learning is a phishing attack. It is a cybercrime that aims to steal sensitive and confidential data such as password, username, banking details from the victims without they even realizing it. This is usually done in the form of fake websites, email spoofing, spear phishing, whaling cross-site scripting, session hijacking, malware phishing, DNS poisoning, or key/screen loggers (Gupta, Arachchilage and Psannis, 2015).

Human beings are considered to be the weakest links in any information security program. The developers, teachers, students, and administrators are the major participants. Lack of information security not only creates issues for them but also affects the credibility of online learning due to proper authentication of students and attribution of student work (Schultz, 2012). Handling of cheating is difficult on such platforms raises a big question. A study done by Northcutt, Ho, and Chuang in 2016 shows that the user may create different accounts such as one as a 'harvester' account that gives users correct answers just by guessing the answers and then getting accessed by the 'Show Answer' button. One can also have a 'master' account that allows submitting the correct test answers.

However, the world cannot stop using technology, and the threats are evitable in the introduction of any system that has been planned and analyzed. In the next section, we will see the risk assessment.

4. RISK ASSESSMENT

Risk assessment, at its essence, is connected with protecting actions to ensure that assets are appropriately distributed in search of achieving business goals. We conducted a formalized risk assessment and compilation that identifies the risks associated with information management at St. P's High school.

Risk	Asset	Threat/Vulnerability	Likelihood	Consequences	Level of Risk
Risk 1	Application server	Unauthorized system access	Likely	Moderate	Extreme
Risk 2	Student Details Database	Information such as student name, contact information, etc., can be accessed by the attacker.	Possible	Major	Extreme
Risk 3	Organizational Policies and Regulations	Ineffective Policies of St. P's High School causes risk as the employees were not well trained.	Possible	Catastrophic	High
Risk 4	IT Nodes and Communication Network	Modifying access points in the network through network injection or spoofing the mac address	Possible	Major	High

Risk 5	Training Program	Inefficient and ineffective information security training could lead to unsatisfactory deployment of the security system. St. P's management is composed of no ICT practitioners and lacked IT employees.	Likely	Moderate	Medium
Risk 6	Maintenance Server	Accessing the maintenance server using the exploit tools such as SQL injection	Almost Certain	Moderate	Medium
Risk 7	Hardware Device(Desktops, Printers)	Controlling the hardware devices such desktops using DOS attack, Trojan horse or installing malware in the system	Likely	Moderate	Medium
Risk 8	Legal issues	St. P's High school and its employees should abide with the Indian National Policy on Information Technology, 2012(NPIT 2012). Failing to abide with the policies and regulations might lead to legal issues	Unlikely	Minor	Low

Impact Consequence

The table below determines the degree of impact/consequence. Each level from one to five is graded according to the magnitude of the effect, financial impact, and IT Failure.

Consequence level	**Description**	**Financial Impact**	**IT Failure**
1	Insignificant	Less than $500	Essential systems inaccessible for less than an hour
2	Minor	Between $1k – $5k	Essential systems inaccessible for several hours

3	Moderate	Between $5k - $10k	Essential systems inaccessible for less than a day
4	Major	Between $10k - $50k	Essential systems inaccessible for a day
5	Catastrophic	Greater than $50k	Essential system inaccessible for more than a day

Risk Matrix

A risk matrix is defined by the equation of likelihood with levels of consequence. The risk rating is calculated using the intersection of likelihood and consequence level. The risk rating is graded into four low, medium, moderate, and catastrophic categories. The overview of each level is presented in the table

Risk Matrix					
Likelihood	Consequence				
	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	Low	Medium	**Risk 6**	Extreme	Extreme
Likely	Low	Medium	**Risk 1, 5, 7**	High	Extreme
Possible	Low	Low	Medium	**Risk 2, 4**	**Risk 3**
Unlikely	Low	**Risk 8**	Medium	Medium	High
Rare	Low	Low	Low	Medium	Medium

Risk Factor	Action
Extreme	The Head of the school and the IT employee must be proactively informed and necessary measures should be taken instantly, with all relevant operations terminated

High	The Head of school and the IT employee must be urgently informed, and appropriate measures need to be taken within 24 hours of an alert.
Medium	The risk information should be provided to the IT employee. The IT employee should monitor the risk, and the preventive measures are taken within three days.
Low	Inform IT employees about the risk. The IT employee shall ensure that preventive measures are taken within one week

5. COMMUNICATION OF RISKS

The recession in recent times that has rattled the St. P's has caused its reputation significantly worse for the public opinion. This has created a situation where the school has not yet regained the student's absolute trust. All of this, along with the development in technology and incident, the challenges faced by the St. P's high school to implement virtual technology, and lack of technical knowledge in employees, is in a precarious state. This report illustrates the critical causes of risks below for a more precise explanation of these findings.

Technical Risks

The St. P's High School faces technical risks such as authentication, availability, confidentiality attacks, and integrity attacks.

Phishing attacks by social media usually include the psychological manipulation of students and employees of St. P's into sending out their personal information. These incidents happen via fraudulent emails that seem trustworthy, where the students end up clicking a fraudulent link or sharing confidential information. The level of this risk is extreme (Thakur & Kaur, 2016).

Denial of Service is implemented to make the assets of networks and systems inaccessible to students and employees of St. P's so that nobody can use it. Attackers could create an environment in which the St. P's high school administrative employees cannot interrupt their process. These attacks' key targets are database servers to obtain information on students and their personal systems (Tripathi & Mehtre, 2013).

SQL injection is a programmer technique for the execution of unauthorized SQL queries on the student database server. It can be performed across a web-based application to obtain confidential information through the St. P's high school databases.

Consequently, the reality that networks and technical systems are being exploited due to current loopholes and lack of adequate security protocols or quality improvement, making it incredibly impossible to prevent cyber attacks.

Operational Risks

Constant access to information focuses on understanding the organizational structure. Also, it relies on how this information within the organization is continuously assessed. Database-based information provides a detailed and enduring plan that will overcome emerging issues.

The primary challenge is from an inadequate general knowledge among employees and students of St. P's and a vague understanding of the challenges that occur during operational activities and the need to respond to cyber threats. With the introduction of new technology to the education system, it is difficult for the students and employees to adapt to the system. This is demonstrated by a difference between the knowledge of the threat from technical experts and the employees without technical knowledge (Hemrit & Ben Arab, 2012).

The risk assessment indicates that high school actually struggle to defend themselves from security threats, and even though employees and students undergo a training program, they are not adequately educated about standard training policies.

The risk assessment analysis shows that this is mostly because employees and students are not aware of security problems, reporting that many of them have not taken some form of training curriculum addressing malware, cyber threats, or effective security policies.

5. RECOMMENDATIONS

Risk mitigation could be stated as taking the necessary steps to reduce the adverse effects. While mitigating risk, this is essential in developing a strategy that relates closely as well as matches the profile of the organization. This is the strategy for preparing for as well as lessening threats' effect, which is faced by the data center. This means reducing the extent of exposure of risk as well as risk's adverse effects. For understanding when risk mitigation could be applied, the process of risk management should be applied. There is a certain procedure of risk management that should be followed. Risks should be identified first. Analysis, as well as deliberation, are required for uncovering, recovering as well as describing risks that could affect the project or the outcomes. Checklists have huge use of value (Panjehfouladgaran & Lim, 2020). They could be helpful to the project team as well as project managers to identify certain risks on the checklist, also expanding the team's thinking. Risks should be appropriately evaluated. Measuring the risks through the dimensions details risk inequality. Few risks could occur more than others, as well as few risks have a greater impact on business operation or project. By measuring the risk-based upon the dimensions, critical risks could be identified which need to be mitigated, here all the risks associated to information management within St. P's High school and for each risk mitigation strategy have been identified.

Risk 1: Application server

Vulnerability: Unauthorized system access

Mitigation: Best practices of user passwords should be enforced, where the users would be forced in selecting long passwords which consists of numbers, letters as well as special characters along with change the passwords frequently. The users should be educated in avoiding use of terms which could be guessed in brute force attack, informing them of updating of routine password as well as telling them in avoiding sharing the passwords over systems.

Risk 2: Student Details Database

Vulnerability: Information like student name and contact name could be accessed by attacker.

Mitigation: Assets should be classified. Classifying the assets defines protection's appropriate level which is necessary for the data set. This would determine cost to secure the assets based upon the value as well as impact they would have (Wong, et al., 2019). Classifying assets fundamentally is prioritizing for determining which assets should be protected first.

Risk 3: Organizational Policies and Regulations

Vulnerability: Ineffective Policies of St. P's High School causes risk as employees were not well trained.

Mitigation: Microlearning approach could be considered and deliver relevant as well as useful content in chunks of bite size. Checklists, short videos and infographics are simple formats of microlearning which make the training much easier for consumption.

Risk 4: IT Nodes and Communication Network

Vulnerability: Modifying access points in network through network injection or spoofing mac address

Mitigation: Strong mechanism of encryption should be applied upon wireless access points which prevents the unwanted users in joining the network. Weak mechanism of encryption could allow hacker to brute force into network as well as begin in modifying the access points within network through network injection or by spoofing the mac address.

Risk 5: Training Program

Vulnerability: Ineffective and inefficient information security training could lead in unsatisfactory deployment of security system.

Mitigation: IT team should be trained on complex solutions of security system, especially if these include recent purchases which are aimed in bolstering the security. IT team would need also training about how satisfactory deployment of security system for closing the vulnerabilities (Soomro, Shah & Ahmed, 2016).

Risk 6: Maintenance Server

Vulnerability: Accessing maintenance server by using exploit tools like SQL injection

Mitigation: Protecting the maintenance server against exploit tools like SQL injections is through filtering the input properly as well as thinking about if input could be trusted. As filtering is quite tough to perform, filtering functions of the framework could be used.

Risk 7: Hardware Device

Vulnerability: Controlling hardware devices like desktops by using Trojan horse, DOS attack or by installing malware within system.

Mitigation: Security of hardware device starts with installing as well as running internet security suite, Diagnostic scans should be run periodically with software. Software of operating system should be updated as well as other software should be checked for updates which are within the system. Email attachments should be careful checked as well as scanned properly.

Risk 8: Legal Issues

Vulnerability: ST. P's High School as well as its employees must abide with Indian National Policy on Information Technology. Failing in abiding with regulations and policies could lead in legal issues.

Mitigation: Sustainable business policy should be built for the employees of St. P's High School as less toxic environment would reduce the compensation claims of the worker (Tom, 2018). Software of risk management should be major priority for the employees of the school.

6. REFERENCES

Arkorful, V., & Abaidoo, N. (2015). The role of e-learning, advantages and disadvantages of its adoption in higher education. International Journal of Instructional Technology and Distance Learning, 12(1), 29-42.

Chen, Y., & He, W. (2013). Security risks and protection in online learning: A survey. International Review of Research in Open and Distributed Learning, 14(5), 108-127.

Gupta, B. B., Arachchilage, N. A., & Psannis, K. E. (2018). Defending against phishing attacks: taxonomy of methods, current issues and future directions. Telecommunication Systems, 67(2), 247-267.

Hemrit, W., & Ben Arab, M. (2012). The major sources of operational risk and the potential benefits of its management. The Journal Of Operational Risk, 7(4), 71-92. doi: 10.21314/jop.2012.115

Kearns, L. R., Frey, B. A., Tomer, C., & Alman, S. (2014). A study of personal information management strategies for online faculty. Journal of Asynchronous Learning Network, 18(1).

Northcutt, C. G., Ho, A. D., & Chuang, I. L. (2016). Detecting and preventing "multiple account" cheating in massive open online courses. Computers & Education, 100, 71-80.

Panjehfouladgaran, H., & Lim, S. F. W. (2020). Reverse logistics risk management: identification, clustering and risk mitigation strategies. Management Decision.

Schultz, C. (2012). Information security trends and issues in the moodle e-learning platform: An ethnographic content analysis. Journal of Information Systems Education, 23(4), 359.

Singh, A., Mangalaraj, G., & Taneja, A. (2010). Bolstering teaching through online tools. Journal of Information Systems Education, 21(3), 299.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215-225.

Thakur, H., & kaur, S. (2016). A Survey Paper On Phishing Detection. International Journal Of Advanced Research In Computer Science.

Tom, M. (2018). Risk Mitigation Strategies in Information Systems Continuity Plans for Public Institutions: The case if Industrial Development Zones (IDZs) (Doctoral dissertation, University of Cape Town).

Tripathi, N., & Mehtre, B. (2013). DoS and DDoS Attacks: Impact, Analysis and Countermeasures. Conference: Advances In Computing, Networking And Security, 2013 TEQIP II National Conference On.

Wang, S., & Heffernan, N. (2010). Ethical issues in Computer-Assisted Language Learning: Perceptions of teachers and learners. British Journal of Educational Technology, 41(5), 796-813.

Wong, W. P., Tan, H. C., Tan, K. H., & Tseng, M. L. (2019). Human factors in information leakage: mitigation strategies for information sharing integrity. Industrial Management & Data Systems.