SECMAN Risk Management and Data Security Essay

Contents

[Introduction 2](#_Toc117889193)

[Risk Management Life cycle: 3](#_Toc117889194)

[Risk identification: 3](#_Toc117889195)

[Threat analysis: 4](#_Toc117889196)

[Threat tree 5](#_Toc117889197)

[Attack tree 6](#_Toc117889198)

[Risk Assessment: 6](#_Toc117889199)

[Quantitative approach: 7](#_Toc117889200)

[Qualitative approach: 7](#_Toc117889201)

[Risk Response and Mitigation 12](#_Toc117889202)

[Counter measures: 12](#_Toc117889203)

[Risk Control Monitoring and Reporting 15](#_Toc117889204)

[ITU-T Cybersecurity Risk Indicator 15](#_Toc117889205)

[KRI values 16](#_Toc117889206)

[Conclusion and Discussion 17](#_Toc117889207)

[References: 17](#_Toc117889208)

[Bibliography 17](#_Toc117889209)

[Appendices 18](#_Toc117889210)

[Appendix A Risk identification table 18](#_Toc117889211)

[Appendix B: Risk Assessment: 19](#_Toc117889212)

[Figure 1 Threat tree 6](#_Toc118590731)

[Figure 2 Attack tree 7](#_Toc118590732)

[Figure 3 Binary risk analysis mapping 10](#_Toc118590733)

[Figure 4 Determining Impact 11](#_Toc118590734)

[Figure 5 Determine impact 11](#_Toc118590735)

[Figure 6 determine risk 12](#_Toc118590736)

# Introduction

Most identify risk with something bad, such as danger and loss. However, there is no universal definition of risk. According to the New Vocabulary of the Polish Language, risks include the likelihood of failure, loss, and actions that might result in such outcomes. In reality, there are two types of risk: The first is a negative view of risk, and the second is a neutral understanding of risk. Examples in the document demonstrate the negative idea of risk. Such a notion is used in insurance, for example, no one here will warn you about the danger of injury as a possibility but solely as a threat. Although the first notion of risk indicates the chance of not attaining the intended outcome, the second concept states that the risk is not just in the setting of risk but also in possibilities. A key feature is to demonstrate the significance of the issues and the correct subject of risk management.

The risk is the state that emerges from uncertainty about the possibility of a negative circumstance occurring that might impact the endeavour. As a result, a project with a high degree of risk is one in which the total evaluation of potential bad effects of hazards exceeds the acceptability limitations.

To provide more course materials, encourage effective learning strategies, and answer questions from students, eLearning professionals are beginning to rely more and more on social networking channels. Additionally, students may communicate with course instructors via social media, ask questions, and get answers to their queries quickly and easily (Mnkandla, 2017).

Today, almost all students have a digital presence. These students often consume material online and are well-versed in the ins and outs of social media platforms. Consequently, social media adoption and integration into education and learning can benefit students.

The use of video lessons, quizzes, tagging, and group discussions by learners are all options available to instructors. In this approach, students will not only learn in a fun & entertaining way, but they will also have the privilege to study whenever and wherever they desire (Alwi, 2010).

Various teachers use social media to help to learn, including sharing educational resources, assigning homework, planning observations and group discussions, encouraging cooperation, & polling students' opinions. However, moving educational activities into a virtual social setting has dangers and unfavourable outcomes. They are numerous and diverse, including applying low-quality digital educational resources, stealing intellectual property, using stolen essences for abusive purposes, harming the reputations of students and teachers, interfering with students' mental health, and others.

To guarantee the standard of teaching and accredit the public schools, the state and the government, who serve as the primary regulator of social processes, exert significant efforts to control the education market. Numerous secondary and higher education teachers utilize social media in the classroom to share learning resources, assign homework, plan observations and discussions, facilitate cooperation, get learner feedback, etc. Similar circumstances apply to coaching, which is not rigorously supervised but is becoming increasingly popular (Almarabeh, 2019).

Information security is a critical threat that might impact universities utilising social media in education. The student and the professor, with their understanding, skills, competencies, & authority , as well as the trust built between them, are at the core of the educational environment. To stop fraud and other nefarious acts by third parties, it is now required to take additional steps to secure confidential info due to the move of schooling to the virtual world.

Due to the high level of trust between students and teachers, the implementation of social media feels that education is even more severe. Generally, it is based on the lecturer's current academic position, experience level, student responsibility, or ability to be trusted. Suppose we apply this faith in social media to online learning. In that case, it may significantly imply that the bulk of malicious activities lurking on the internet may be easily transferred to students, professors, schools & universities.

In this essay, we investigate & evaluate four areas of risk management:

1. Identification

2. Assessment

3. Response & mitigation

4. Monitoring & reporting

These four categories will be evaluated regarding the danger they pose to online web portals elearning for students.

# Risk Management Life cycle:

We perform risk management in an e-Learning system, i.e., the goals that support the choice to invest in an e-Learning system and abandon the traditional teaching method. The most crucial goal of an effective e-Learning system is the progressive progression from essential information-supply tools to the next level of employing interactive tutorials and then to collaborative technology to encourage creativity, collaboration, communication, and research skills (Rossi, 2007). Starting with this primary goal, we divided the risk management life cycle into following steps.

## Risk identification:

Every component of the lowest level of risk will be chosen to create interview questions for the risk identification process. Risk is uncertainty's potential positive or negative impact on the e-learning goal. If a risk identification, it might improve, hinder compromise, hasten, or postpone the attainment of goals (Tchankova, 2002).

### Threat analysis:

The relevant probable threat-sources & related threat behaviors that apply to the E Learning were found.

Table 1. **Threat analysis table**

|  |  |
| --- | --- |
| **Threat-Source** | **Threat Actions** |
| **Hackers** | * Web defacement |
| * Social engineering * XSS * Sensitive Data exposure * Weak Access Contorl * SQl injection * Unauthorized web access * Phishing |
|  |
|  |
| **Student threat** | * Fraudulent act |
| * Spoofing |
| * Information bribery |
| * System intrusion * Man in middle attack |
| **Insiders** **University of Portsmouth Threat** | * Remote code execution |
| * Ego |
| * Computer abuse |
| * System bugs |
| * Malicious code(e.g. virus, Trojans etc) |
| * Blackmail |
| **Teacher threat** |  |
| * viruses, at the time of receiving e-mail or by running different software on that computer * LMS or CMS  damages occur when receiving messages or using other applications on that machine. |
| * Malware |
|  |

**List of all assets:**

Consider all internal and external assets, including but not limited to:

* + People
    - students, teachers, managements, visitors
  + Customers
    - Contact and purchase information
  + Technology
    - IT systems, networks, communications, servers, websites, plug-inn, database
  + Information
    - Employee PII, business sensitive or proprietary, credit card information
  + Systems
    - Alarm, SCADA, Mysql
  + Processes
    - Online e learning, social media

### Threat tree

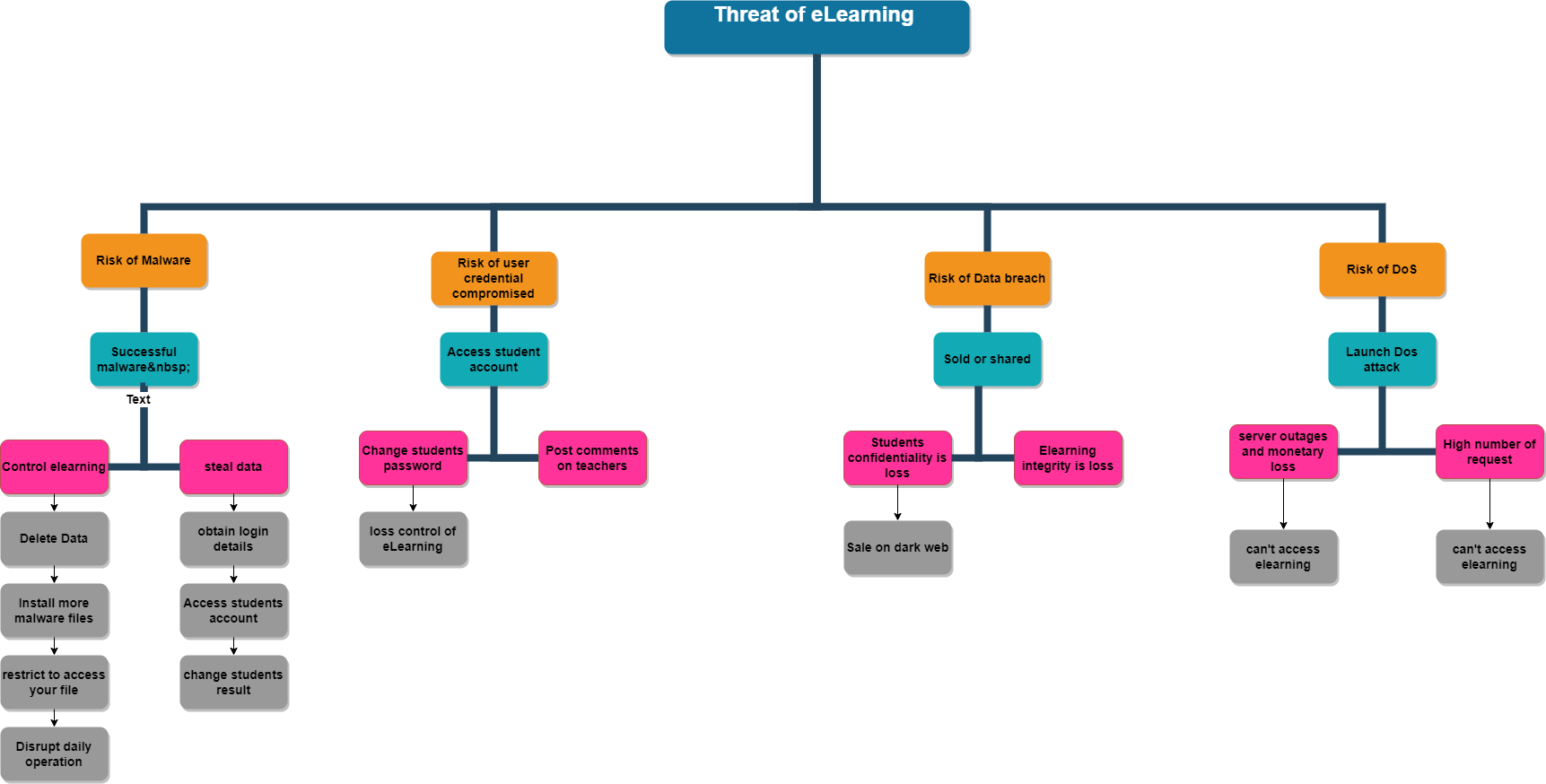


Figure 1 Threat tree

It is clear that, even though the main four were picked for further risk investigation when examined, they might have various paths and actions that negatively influence the platform. The impact ranges from elearning & cybersecurity-related behaviors like viruses show in figure 1.

### Attack tree

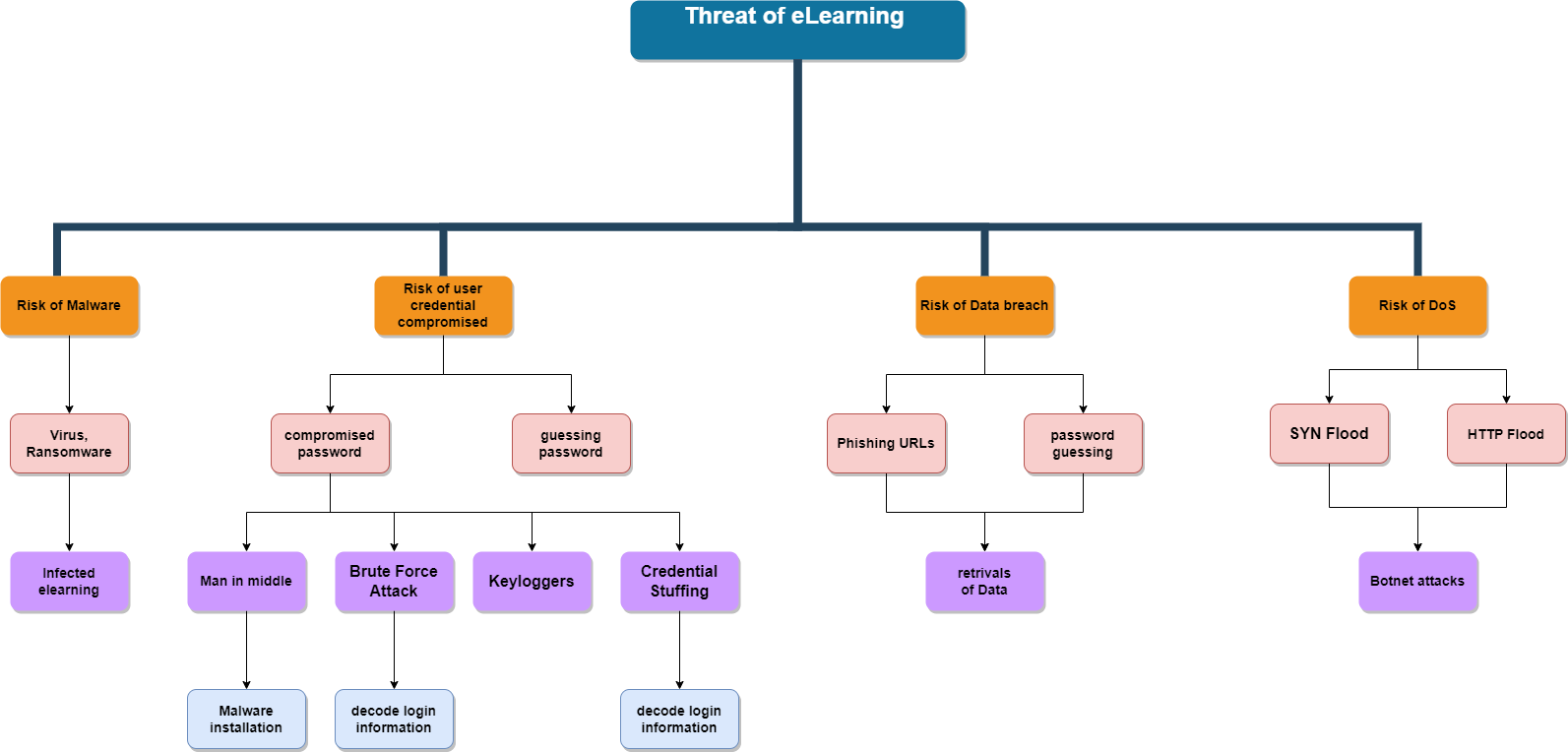


Figure 2 Attack tree

## Risk Assessment:

Risk assessment is a topic that researchers have emphasized on recently. We will go in details.

Table 2 . risk assessment types

|  |  |
| --- | --- |
| **Qualitative** | **Quantitative** |
| SWOT | CPM |
| Check list analysis | PERT |
| Documents Review | Sensitivity analysis |
| Brainstorming | Numerical |

### Quantitative approach:

It is used to anticipate prospective project schedules and cost results, providing the corresponding confidence level for each possible value of the taken-into-account value (Dvorak, 2020).

As a result, the potential values of a particular variable are described in terms of a probabilistic distribution (impact areas). If more precise statistics are not available, all that is needed is to quantify the tiniest, most probable, and maximum values the variable may have.

In order to calculate the total effect, quantitative risk analysis ranks hazards from high, medium, & low to real the values and probability of occurrence (Sperber, 2001).

In this essay, we conduct a binary risk assessment, which asks seven questions with yes or no responses, can be performed. These may be entered into a matrix to calculate a specific danger's likelihood, effect, & risk. The assessment of the risk of compromised credentials is provided below.

### Qualitative approach:

Interviews are one of the numerous techniques used to carry out qualitative risk identification analysis, and they may be utilized to provide adequate risk statements for a particular project. Participants in the eLearning, including teachers, senior professors, chiefs, vice chiefs, heads of academic programmes, & students, provided risk statements for this study. For each Risk aspect, direct or virtual interviews were carried out to create risk statements. Every released statement must adhere to the financial risk management concept to guarantee the research statement's accuracy. To prevent confusion between cause and risk, the meta-language rules referred to as "conditional statements" or "condition-consequence risk statement" will be implemented first. Any assertion that does not fit these requirements will be disregarded. Second, there should be a connection between the meta-language and the distinctions between risk and assumption. Known limits restrict the presumption statement, yet there are unknown dangers and regulations in the future. As a result, claims to have clear implications for the future will also be dropped. All students-registered threat were compared using the data sources triangulation approach to guarantee the authenticity of each claim (Rot, 2008).

We used the following risk identification methodology to identify threats related to the elearning network that an online service that enables students to learn from elearning:

R = T x I where x = multiplication

R = Risk

T= Threat

I = Impact

Table.3 Binary risk assessment of compromised credentials

|  |  |  |
| --- | --- | --- |
| **No** | **Questions** | **Response** |
| 1 | Can the attack be completed with common skills? | No |
| 2 | Can the attack be completed without significant resources? | No |
| 3 | is the asset undefended? | YES |
| 4 | Are there weaknesses in the current defences? | Yes |
| 5 | is the vulnerability always present in the asset? | No |
| 6 | Can the attack be performed without meeting any significant preconditions? | No |
| 7 | Will there be consequences from internal sources? | YES |
| 8 | Will there be consequences from external sources? | NO |
| 9 | Does the asset have a significant business value? | No |
| 10 | Will the asset have a significant cost of repair or replacement? | YES |

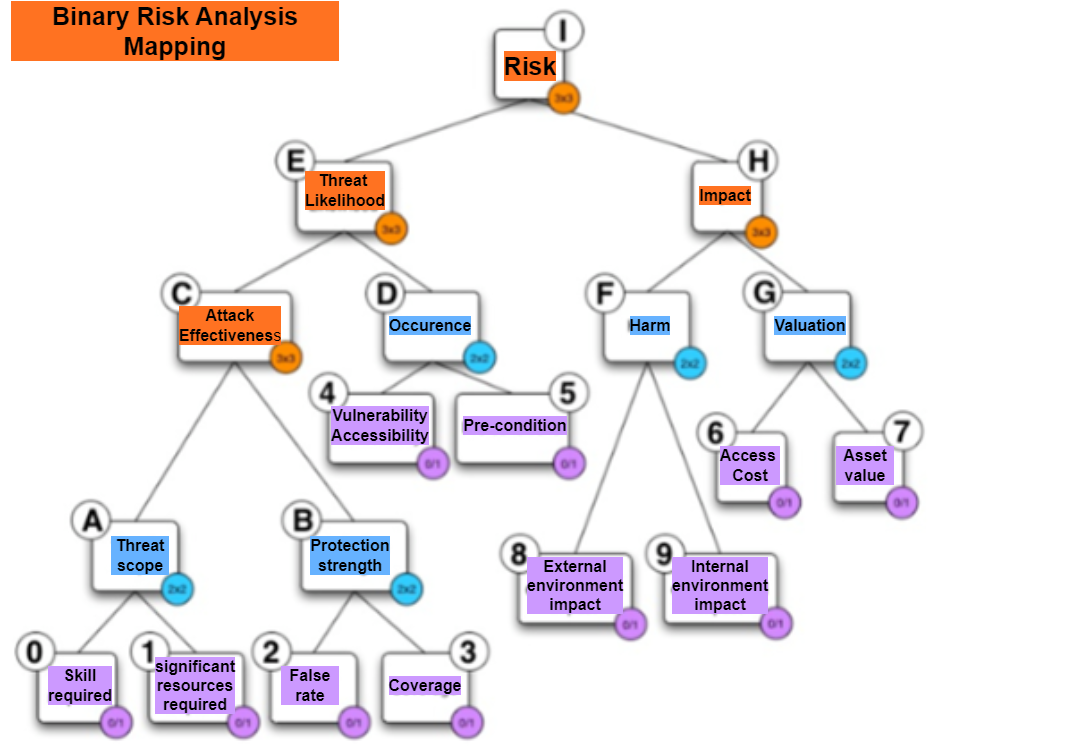
****

Figure 3 Binary risk analysis mapping

**Step 1: Determining Impact**

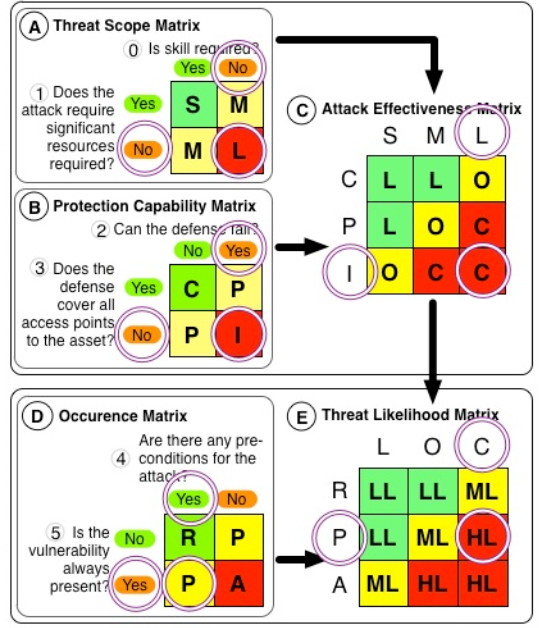


Figure 4 Determining Impact

**Step 2: Determine impact**

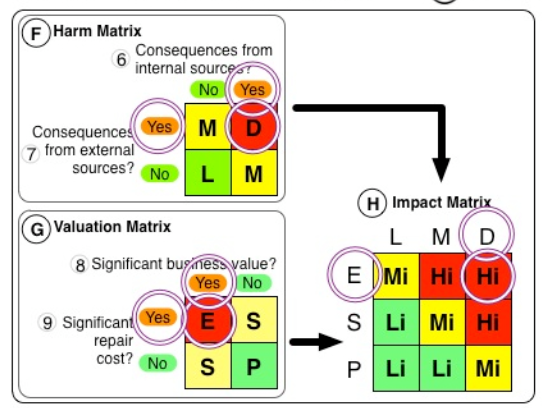


Figure 5 Determine impact

Step 3: Determine Risk

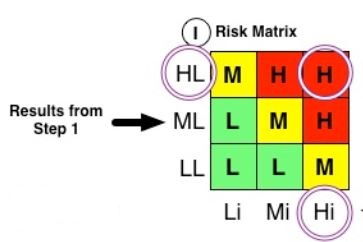


Figure 6 determine risk

In this we noticed that some of the rational are subjective.

* Risk: High
* Likelihood: High
* Impact: high

# Risk Response and Mitigation

A procedure for modifying or responding to a risk. Acceptance, avoidance, mitigation, or sharing are all options for risk response. After reviewing and addressing the dangers associated with the eLearning system, solutions should be provided. The list of solutions for the online learning system is as follows:

1. Accept the Risk
2. Avoid the Risk
3. Mitigate the Risk
4. Transfer the Risk

Risk avoidance strives to eliminate the possibility of a risk occurring and its capacity to negatively affect the company. The goal of risk reduction is not to destroy the case of a threat but rather to reduce its impact to an acceptable level.

Risk acceptance leads to risk mitigation. You understand that risk may influence your company and put plans and actions in place to limit its impact. You do not avoid danger. Instead, you accept the risk, proceed with the activity, and devise a mitigation strategy to mitigate the risk's potential negative repercussions.

## Counter measures:

We used the risk matrix to determine whether it was worth protecting against & developed countermeasures. A countermeasure matrix is used to estimate the efficiency of the countermeasures against the specified risks; by operating the rate of decrease & likelihood, we may obtain an outcome that helps us make YouTube safer.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Countermeasure | Risk of malware | Risk of user credential compromised | Risk of Data breach | Risk of DoS | Combined countermeasure |
| Strong privacy setting  Cost = 0.5 | Reduction = 0.8 | Reduction = 0.2 | Reduction = 0.85 | Reduction = 1 | 1.82 |
| Firewall deployment  (cost = 0.2) | Reduction =0.8 | Reduction = **1** | Reduction = 1 | Reduction = **0.1** | 1.92 |
| Effective reporting system  Cost = 0.1 | Reduction = 0.35 | Reduction = 0.5 | Reduction = 0.9 | Reduction = 0.7 | 1.90 |
| Strong authentication and passwords  Cost= 0.5 | Reduction = **0.9** | Reduction = **0.1** | Reduction = **0.9** | Reduction = **0.9** | 1.8 |
| Combined Risk Reduction | 0.9976 | 0.9784 | 0.9664 | 0.9675 |  |

Table.4 Risk Countermeasure Matrix.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat** | **Vulnerability** | **Asset and Consequences** | **Risk** | **Mitigation** |
| System failure – overheating in server room  High | Air conditioning system is ten years old  High | Servers and service es unavailable for 3 hours  Critical | High  Potential loss of $50,000 per occurrence | Buy a new air conditioner. Cost approx. $3,000 |
| Web defacement  Low | Gaining unauthorized access to a web development.  Low | Can’t access the web portal for 4 hours  Low | Client loss of $20,000  Low | 24/7 monitoring  Cost- $10,000 |
| Sql injection  High | to acquire databases, alter material, steal data, or introduce malware, you may inject harmful code into any website's pages.  High | All files and folders are deleted for 7 hours  Critical | Financial loss $ 5000  High | Use sql queries, character escaping, xss, data cleaning, and web-based firewalls. Don't link your database to a user account with administrator privileges.  Cost $ 70000 |
| XSS  High | may be used to steal user passwords, hijack sessions, as well as get around multi-factor login.  High | Can’t access own web page for 2 hours  Critical | Potential loss of $3000  High | Use algorithms which block XSS  Cost $9000 |
| **Sensitive Data Exposure**  Moderate | breaking into software and networked systems  Moderate | Not access to system for 6 hours  Moderate | Financial Loss of $6000  High | Use effective encryption techniques to shield the data from unauthorised access.  $11000 |

**Table.5: Risk countermeasures with Risk Mitigation Strategy Packages**

We also used countermeasures within the threat tree produced during the risk identification step. This may give more intricacy to the threat tree & is an excellent way to examine how different countermeasures can reduce many threats.

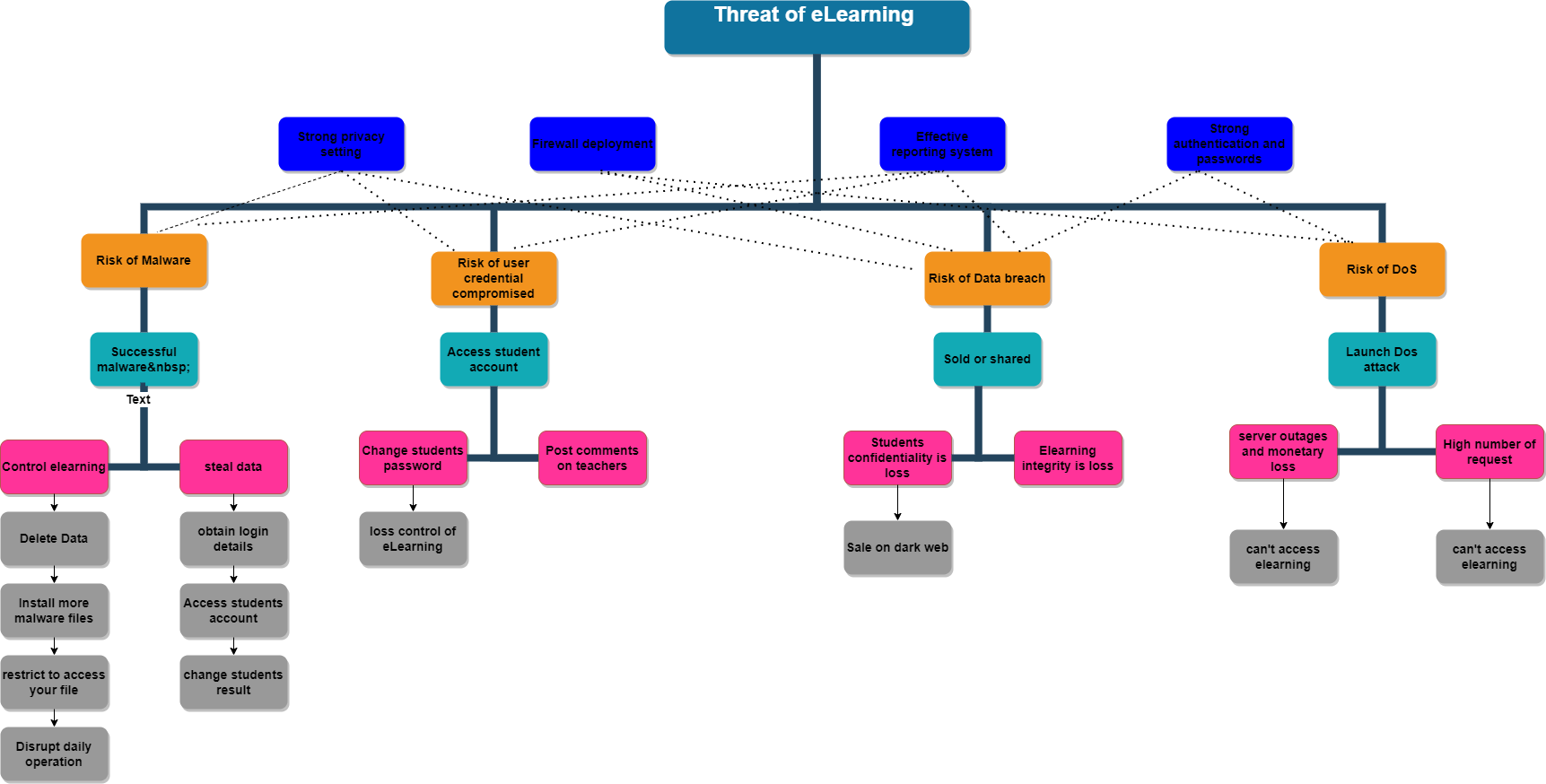


Figure Threat Tree with Countermeasures

# Risk Control Monitoring and Reporting

The practice of conveying real-time risk and performance data to various stakeholders is known as risk reporting. Monitoring risk is a constant activity that leads to a better understanding of what is happening across multiple company sectors. Monitoring risk over time allows management to:

* Determine crucial trends
* Respond appropriately and efficiently identify business opportunities
* process improvements that would not have been visible without adequate monitoring

## ITU-T Cybersecurity Risk Indicator

Three critical indicators are chosen for two months to continue the monitoring process, & the KRI values are generated using the relevant indicator data. Which may then be further analyzed. The relevant indicators listed below have been chosen (ITU, 2020).

* Server failures:

( no.of server failures / no. of server failure soved within 24 hours) x 100

* Incidence response indicator:

(Number of incidents reported / Total number of incidents reported within 24 hours) x 100

* Account logins:

(No. of login/ No. of successful logins) x 100

### KRI values

Table.6 KRI values

|  |  |  |
| --- | --- | --- |
| KRI/Month | 1 | 2 |
| Server failures: | 78% | 85% |
| Incidence response indicator | 89% | 76% |
| Account logins | 96.3% | 98.2% |

Figure KRI performance graph

# Conclusion and Discussion

Three essential risk variables that may have happened during the online education project execution in Indonesia were identified due to this risk assessment. However, a risk assessment analysis revealed three critical risks: unstable Internet connections, unfavourable learning environments, and changes in tuition fees. These three hazards were chosen because they had the highest likelihood and impact severity scores in the P-I analysis, which respondents believed to be the most significant dangers.

The potential dangers that may arise for various E-Learning participants and tools and approaches that may be used to mitigate such risks. Nevertheless, with electronic learning, only students decrypt their private information; the remaining difficulties lie in implementing and maintaining greater confidentiality when establishing the teaching process. The IT department constantly aspires to Utilise redundant hardware such as servers, routers, and other devices to help ensure service availability. Logs are a significant component that further reduces risks. The transaction's specifics, including the time it happened, would be "recorded," and the resulting record would be encrypted using cryptographic methods. Although no system can be completely safe, we may increase the degree of security in e-learning by using additional strategies to reduce the risk. Inaccurate or irrelevant material will cause readers to lose faith in the texts or to stop reading altogether. Therefore, readers must be able to rely on the accuracy of the material. Although risk management is complex, the more projects we complete, the sooner we can effectively detect risks, assess them, and lessen their impact.

# References:

# Bibliography

Almarabeh, H. a. (2019). The impact of cyber threats on social networking sites. *International Journal of Advanced Research in Computer Science 10, no. 2*.

Alwi, N. H.-S. (2010). Threats analysis for e-learning. *International Journal of Technology Enhanced Learning 2, no.4*.

Dvorak, Z. D. (2020). Qualitative approach to environmental risk assessment in transport. *International Journal of Environmental Research and Public Health 17, no. 15*.

ITU. (2020). Retrieved from https://www.itu.int/rec/T-REC-X.1208/en

Mnkandla, E. a. (2017). The use of social media in e-learning: A metasynthesis. *International Review of Research in Open and Distributed Learning: IRRODL 18, no. 5 (2017):*.

Rossi, P. &. (2007). Supporting Project Management Processes with integrated Software tools and database. *PMI EMEA Global Congress, Budapest.*

Rot, A. (2008). IT risk assessment: Quantitative and qualitative approach. *Resource 283, no. March (2008): 284.*

Sperber, W. H. (2001). "Hazard identification: from a quantitative to a qualitative approach. *Food Control 12, no. 4* .

Tchankova, L. (2002). Risk identification–basic stage in risk management. *Environmental management and health*.

# Appendices

## Appendix A Risk identification table

|  |
| --- |
| **Impact** |
|  | **Hackers** | **Computer criminal** | **Insiders Adelaide Threat** | **Terrorist** |
| High 4 | XSS  Sensitive Data exposure  Weak Access Contorl  SQl  Injection  Software attacks | Fraudulent act  System intrusion | Remote code execution  Computer abuse  Malicious code(e.g. virus, Trojans etc) | System penetration  System failure  DoS |
| Moderate 3 | Social engineering | Spoofing | Ego | Earth quake |
| Low 2 | Web defacement | Information bribery | Computer abuse | System tampering |
| Very Low 1 | Virus | APT | System bugs  Blackmail | Fire |

## Appendix B: Risk Assessment:

**Risk Assessment**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **S.No** | **Observation** | **Threat-Source** | **Existing controls** | **Likelihood** | **Impact** | **Risk Rating** | **Recommended** |
| 1 | Passwords are submitted unencrypted over the network | Hackers | HTTP enabled only. | High | High | High | requires the search engine & server to communicate in an encrypted manner.  Cost = $5000 |
| 2 | Insecure HTTP cookies | Hackers | HTTP enabled only. | Medium/  Moderate | Medium/  Moderate | Medium/  Moderate | Fixing the web browser so that all sensitive cookies are set with the Secure, HTTP.Only flag  Cost= $600 |
| 3 | Communication is not secure | Hackers | HTTP enabled only. | Medium/  Moderate | Medium/  Moderate | Medium/  Moderate | Reconfigure the web server to use HTTPS  Cost = $400 |
| 4 | Server software and technology found | Hackers | None | low | low | low | Recommend to remove data such as HTTP server header, HTML meta content, and others that can be used to identify a server, os, technology, or programming environment.  Cost = $ 7000 |
| 5 | Missing HTTP security headers | Hackers | None | low | low | low | 1) Recommend to add the X-Frame-Options HTTP response header to every page that you want to be protected against Clickjacking attacks. |
| 2) Set the X-XSS-Protection header to "X-XSS-Protection: 1; mode=block". |
| 3) Set the X-Content-Type-Options header to "X-Content-Type-Options: nosniff".  Cost = $300 |
| 6 | Password auto-complete is enabled | Hackers | Password should be alphanumeric | low | low | low | It is advised to put the attribute record or information" on all password fields to prevent the login forms' login dynamically feature.  Cost = $ 200 |
| 7 | Remote code execution | Insider threat | None | low | low | low | Upgrade version of apache tomcat.  Cost = $3500 |
|
|
| 8 | Phishing | Hackers | None | Medium/Moderate | Medium/  Moderate | Medium/  Moderate | Keeping Updated With The Latest Phishing Techniques.  Cost = $ 4000 |