Security Risk Management of an Educational Institution: Case Study

[1]Bayenah Almarri, [2]Fatimah Alraheb, [3]Shahad Alramis,
[4]Noor Almilad, [5]Ezaz Aldahasi, [6]Azza Ali

Computer Science Department, College of Science and Humanities,
Imam Abdulrahman Bin Faisal University, P.O. Box 31961, Jubail, Saudi Arabia

Abstract
This study is conducted with an educational institution to minimize the potential security hazards to an acceptable level where the vulnerabilities and threats are revealed in this institution. The paper provides a general structure for the risk management process in educational institutions, and some recommendation that increases security levels is presented.

Key words:
Risk management; risk identification; Education; risk; security.

1. Introduction

With increasing development of technology, computing and network applications have become a part of many institutions such as the educational institution. Risk management mechanism measures hazard protection performance [1]. The risk framework must include management policies and rules for communicating emerging risks and the efficacy of risk management at all enterprise levels to support an efficient risk management process [2]. There are risk assessment steps as shown in figure.1 [3].

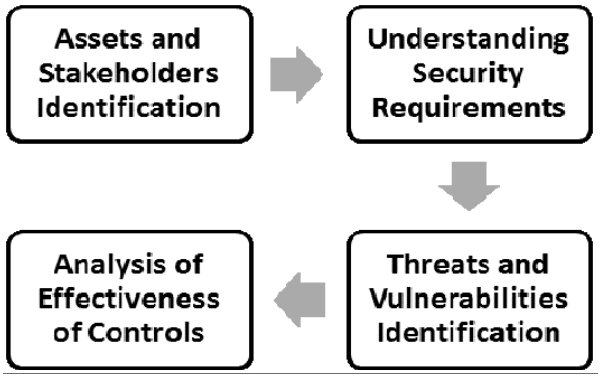
Assets and Stakeholders Identification
Understanding Security Requirements
Threats and Vulnerabilities Identification
Analysis of Effectiveness of Controls

Fig.1 Steps in risk assessment

Risk management is the systematic method of control aimed at identifying all the risks that affect the organizations then determining what to do and how to treat it. The risk management process composed of 4 phases [1].

Figure 2 explains the Risk management process framework in an educational facility.

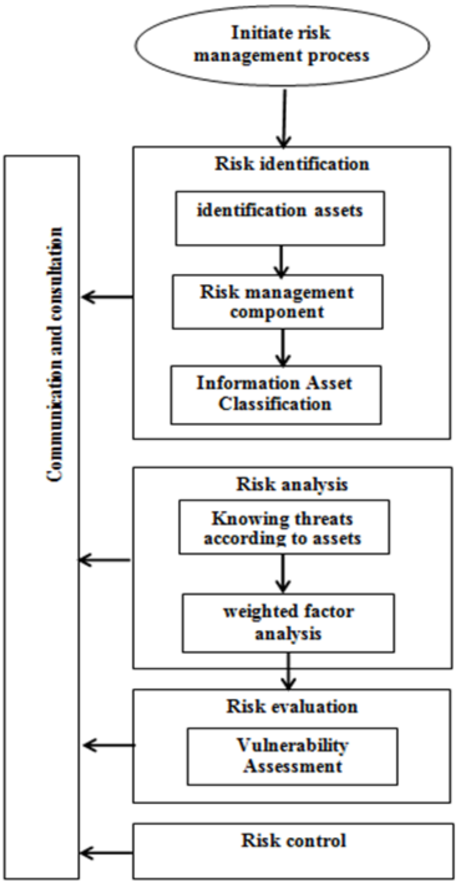
Initiate risk management process
Communication and consultation
Risk identification
identification assets
Risk management component
Information Asset Classification
Risk analysis
Knowing threats according to assets
weighted factor analysis
Risk evaluation
Vulnerability Assessment
Risk control

Fig.2 Risk management process.

1.1 Risk Identification

This is the first stage of the methodology designed to discover all the threats facing the company, regardless of

Manuscript received March 5, 2021
Manuscript revised March 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.3.23

the chance of their occurrence [9]. The owner must make sure that enough and sufficient risk assessment is carried out and detected it earlier, the preparations will decrease the risk and handle it well. The step of risk identification must made it continuously. Risk identification contains the following steps:

1.1.1 Identification Assets

Includes elements such as people, procedures, data and information, hardware, software, and networking.

1.1.2 Information Assets Classification

In this step, the information assets will be categorize based on their sensitivity and security needs. The data classification includes (Public-Private - Confidential).

Public-The lowest classification level, the disclosure of which does not have significant negative implications for the organization.

Private-Only data for internal usage, which is of considerable importance, and its release can negatively affect an entity. All data and information gathered inside an organization should only be handled by employees and should not fall into outsiders' hands.

Confidential-In this classification system, the highest level is. This is susceptible data. Access to confidential information is restricted to those who have a legitimate purpose for accessing such information.

Impact - A risk, by its very nature, always negatively impacts. will be identified impact to profitability such as "high/medium / Critical."

High: The event has a reasonable chance of occurring, it should be regularly discussed, and mitigation actions are taken.

Medium: The event has a normal chance of occurring, and the project team should be aware of it.

Critical: The event's occurrence should be actively managed, and mitigation actions are taken.

1.2 Risk Analysis:

Risk analysis is the review of risks related to a specific action or event. The risk analysis is relevant to IT, projects, security problems, or events based quantitatively and qualitatively. This step contains:

- Knowing threats according to assets.
- Weighted Factor Analysis.

1.3 Risk Evaluation:

At this phase, the resulting risk level is linked to the risk acceptance criterion and identifies risks that may or may not be appropriate [10]

Risk assessment is one of the most important educational tasks.

$$(A * P) - C + V \qquad (1)$$

Where:
A: Asset value
P: Probability
C: Current controls
V: Vulnerability

1.4 Risk Control:

This is the last step of the methodology; it is one of the risk response strategies after analyzing the risk, we must decide what to do with them
There are four possible responses to risks :Avoid the risks; Risk transfer; Reduce the risk; Accept the risk. However, the risk management process must culminate with a list of risks and the mitigation strategy assigned to each risk.

Risk management is a process of identifying and assessing the risk of resources losses, and but a control rules to decreases the failures or losses. This paper's main idea is to address the potential security risks in educational institutions in an organized and systematic way before they occur. This paper presents security risk management concepts and offers the most apparent risks which educational institutions can face. In a particular, the risks were studied in an educational institution and identified the most prominent assets in this institution and the most common threats that need to be controlled. Risk management involves assessing each goal's risk level and calculating the risk analysis by applying different methods and technologies.

2. Related Work

In [4], authors have considered the methods for quantitative information security risk assessment and management in the university telecommunication networks. The authors used fuzzy logic, questionnaires, analytic hierarchy process, and fuzzy prediction rules for risk factors evaluation. The results defined the first serious risk in university is Virus infection for the hosts, and the second one is Phishing. Then authors provided some solutions, such as buying a good anti-virus product. The authors presented results that can be used for information security risk management in the telecommunication network. There is a study that revealed complex risks in academic sites and activities [5]. The authors improved life safety in the university environment by collecting data through detailed health, safety, and environment checklist in 38 different sites and applied a procedure to identify hazards, consequences, and risk evaluation. Hence, the risks quantified, prioritized, and control measures proposed accordingly. As a result, facilities and functions within laboratories, library, and powerhouse were more vulnerable to serious risks as the Chi-square and correlation tests assessed how environmental factors were associated with hazard consequences. In [6], authors find on the relationship between accidents in academic laboratories and the institutions' safety climate at several public higher education institutions in Northwest Mexico. Also, the authors provided a tool that can be used to obtain information to know. They understood the student's point of view about the safety climate in higher education institutions, especially in the laboratory areas. As they estimated, this may help decide whether to adopt preventive measures to improve a real safety climate at universities. This work confirms that the absence of institutional safety commitments contributes to increased laboratory accidents. Authors in [7] provided a data set of a practical method to health, safety, and environmental risk assessment to assess and rank potential threats/hazards, and prevent and decrease the accidents and harmful consequences at an academic setting. Also, they applied descriptive statistics and analytical tests on this data. The data set presents some information about prioritizing determined risks according to the relevant scores and levels for using the control measures to mitigate the related risks. In [8], authors considered assessing the hazard exposure in education institutions and how to determine the possible risk level. The determination of risk rank is measured based on the formula likelihood multiply severity, and the rank needs to refer from the risk matrix standard. As a result, they showed the high, medium, and low-risk levels and found the higher level of risk was in the playing field and hazard in office.

Most of papers, several hazards need to be controlled by education management to avoid the increase of case accident in education. Further studies recommended the most importance of measuring the security risks in the education institutions. Also clarifying risk assessment methods and explaining the process of implementation are recommended. So, in this paper, a case study for an educational center will be presented, and risk assessment for it will be studied. Finally, recommendation that mitigates the risk will be illustrated up on the detailed of the risk assessment report.

3. Methodology

The data related to assets in the educational institution is collected through an interview with an educational institution, and then the security risk management component step is evaluated up on the collected information. The assets in this institution are identified as follows:

- People.
- Procedures.
- Data.
- Software.
- Hardware.
- Networking

Also, each asset's components were as shown in TABLE I.

4. Results

As first, information asset classification for the most critical information for each asset in the educational institution is determined, and then this information is classified based on their sensitivity, security needs to private or public, confidential and based on their impact on establishment profitability to high or medium or critical. TABLE II illustrated the most information asset classification for the educational institution. Secondly, each category's weight is calculated based on the answers to the questions that were asked during the interview with the institution. Thus, the extent of each asset's relative importance is calculated using the analysis of the weighted factors. The ratios ranged between 0.3 – 0.8, as in TABLE III.

After that, the risk estimates are calculated as the expectations of the chance of occurrence of risks and the extent of the impact of these risks if they occur.

They are used to manage risks, and we use them to take this into account. The results are as follows by applying Eq.1:

The first factor: (50*0.5) -30%+70%= 35

The second factor: (71* 0.7)-40%+60%=59.64

In the third factor: (27*0.3)-50%+50%=8.1

In the fourth factor: (47*0.5)-3 0%+70%=32.9

In the Fifth factor: (50*0.6)-40%+60%=36

In the Sixth factor: (37*0.4)-0%+100%=29.6

TABLE I. Risk management component

IT system component:	*Risk management component*	
People	People inside an Organization	Employees (Administrators, teachers) Students. Accounting Department.
	People outside an Organization	Parents. School guard.
Procedures	Procedures	Only one teacher in IT.
Data	Data/ Information	Electronic cloud. Paper archive.
Software	Software	Electronic cloud. ClassDojo platform. Website.
Hardware	Hardware	Desktop computer. Printer. -iPads.
Networking	Networking components	Wi-Fi device. Router device.

5. Discussion

Providing information security and data protection is a critical activity for the current telecommunications networks of different companies like Education. Our study of the educational institution found that the facility does not have anti-virus software on devices. Hence, the activity that needs to be done to increase the institution's security and risk management is to buy a good anti-virus product as it was used in study [11]. As it became clear to us in calculating the risk of Wi-Fi penetration and unauthorized access to the network. Because the risk value is high, that means the need to increase the network protection by monitoring it. It became clear that the foundation is in urgent need of a specialized Information Technology (IT) team to develop alternative plans for any emergency. An Intrusion Detection System (IDS) can be used to increase security in the organization as a detection mechanism used to detect security violations.

TABLE II. Information asset classification

Information assets:		*Data classification:*	*Impact to profitability:*
1.	Entering and following student records	Private	Medium
2.	Send a report to parents	Private	Medium
3.	Accounting department workstation	Confidential	Critical
4.	Entering and updating Employees Information	Private	Medium
5.	Share files between teachers	Public	Medium
6.	Send administrative reports between administrators	Confidential	High
7.	Institution annual plans	Public	Critical
8.	Router Password	Public	Critical

6. Conclusion and Future Work

The purpose of this research was to assess the security risks in educational institutions, and the result based on an assessment of the value of the risk was the need in educational institutions to increase protect the Internet and Wi-Fi resources from permeation that then lead to unauthorized access. Based on the results, there was a need for a specialized IT team to be responsible for following up on hardware maintenance, network protection, and increased technical efficiency of the organization.

Finally, a recommendation for IT team applies practical tools by examining networks through programs to check networks, discover security vulnerabilities in them, and then match the empirical results with the theoretical results that we reached. Also, the educational institution should to have an alternative plan is appropriate for any emergency situation in the organization, enabling it to control risks or mitigate risks.

TABLE III. Weighted factor analysis

Information assets:		***Impact on Revenue***	***Impact on Profitability***	***Impact on Public Image***	***Weighted Score:***
Criterion weight (1-100)		**30**	**40**	**30**	**100**
1.	The lack of alternative plans for any emergency	0.4	0.5	0.6	50
2.	Wi-Fi penetration and unauthorized access to the network.	0.6	0.8	0.7	71
3.	Ease of access to data stored in paper archive.	0.2	0.3	0.3	27
4.	No anti-virus software on devices	0.4	0.5	0.5	47
5.	Lack of IT professionals.	0.6	0.5	0.4	50
6.	Lack of controlling and monitoring by a network	0.4	0.4	0.3	37

References

[1] Zavadskas, E. K., Turskis, Z., & Tamošaitiene, J. (2010). Risk assessment of construction projects. Journal of civil engineering and management, 16(1), 33-46.

[2] Culcleasure, F. D. (2005). Risk management: A study of current practices at north carolina's private colleges and universities.

[3] Joshi, C., & Singh, U. K. (2017). Information security risks management framework–A step towards mitigating security risks in university network. Journal of Information Security and Applications, 35, 128-137.

[4] I. V. Anikin, "Information security risks assessment in telecommunication network of the university," in 2016, DOI: 10.1109/Dynamics.2016.7818967.

[5] A. Dehdashti et al, "Applying health, safety, and environmental risk assessment at academic settings," BMC Public Health, vol. 20, (1), pp. 1328-1328, 2020.

[7] A. Dehdashti et al, "Data of risk analysis management in university campuses," BMC Research Notes, vol. 13, (1), pp.

[8] A. R. Ismail et al, "Risk assessment in infrastructure in educational institution: A study in Malaysia," IOP Conference Series. Materials Science and Engineering, vol. 257, (1), pp. 12056, 2017.

[9] Raanan, Y. (2008). Risk Management in Higher Education: Do We Need it? Risk Management in Higher Education, 1000-1007.

[10] Henriksen, E., Burkow, T. M., Johnsen, E., & Vognild, L. K. (2013). Privacy and information security risks in a technology platform for home-based chronic disease rehabilitation and Education. BMC medical informatics and decision making, 13(1), 85.

[11] Anikin, I. V. (2016). Information security risks assessment in telecommunication network of the university. Paper presented at the 1-4. doi:10.1109/Dynamics.2016.7818967.