Recommendations for Risk Analysis in Higher Education Institutions

Lidia Prudente Tixteco, María del Carmen Prudente Tixteco, Gabriel Sánchez Pérez, Linda Karina Toscano Medina, José de Jesús Vázquez Gómez, Arturo de la Cruz Tellez
Instituto Politécnico Nacional
Sección de Estudios de Posgrado e Investigación ESIME Culhuacan
Santa Ana 1000, San Francisco Culhuacán, Coyoacán, D. F., México
email: lprudente@ipn.mx, mprudentet0900@alumno.ipn.mx, gasanchezp@ipn.mx, ltoscano@ipn.mx, jjvago@gmail.com, adelacruzt@ipn.mx

Abstract— **Computer attacks do not only happen in large companies or organizations. Educational Institutions have also started to become aware of computer threats to which their information assets are exposed. Among these institutions, universities, higher education and research centers are the most at risk, because they handle information regarding scientific and technological research and/or developments, personal data of their staff and students, academic records, and many others. A risk analysis is one step to start an information security strategy. It allows assessing the risk of information assets in order to know their security status, and helps to define a security controls implementation plan to avoid threats that exploit some vulnerability that could cause serious damage to an asset or infrastructure of *Higher Education Institutions* (*HEIs*). This paper presents some recommendations to perform a risk analysis in *HEIs* to identify threats and helps to reduce the risk of their information assets.**

Keywords-risk analysis; higher education institutions; information systems.

I. INTRODUCTION

Large companies or organizations are not the only ones concerned about their information assets security. Educational institutions are also becoming aware of the risk of incorporating information systems into their daily processes which makes them vulnerable to threats. Under these circumstances, implementing an information security strategy is required to help handle potential threats and reduce the risk of the information assets of the educational institutions.

Information Systems (*IS*) are used to contribute in education field, but they introduce more risks to educational processes. Information Technologies (*IT*) support *IS* and they could have some vulnerabilities that may compromise confidentiality, integrity and availability of the systems and their information. In 2014, the Organization of American States (*OAS*) and Symantec Corporation published the Cyber Security Latin America and Caribbean Report [1], which shows the extent of the cyber security incidents reported to the Mexican Federal Police against different entities. The report shows that 31% government institutions, 26% private sector institutions, 39% academic organizations and 4% other entities were affected.

Information security constitutes an important element for Higher Education Institutions (*HEIs*). Due to the use of Information Technologies (*IT*), the number of information security incidents in academic environment has increased, and these institutions need to implement a good information security management to protect their information assets. However, this can be difficult to accomplish [2].

A risk analysis is an objective and efficient way to start an information security strategy design, which allows to assess the risk of information systems. It helps to identify the security level of the critical assets and determines a security control implementation plan in order to reduce threats probability and attacks that can cause major damages to an organization [8].

In *HEIs*, it is unwise to implement controls or safeguards just because they seem to be the right thing to do or because other entities or organizations are doing so. Each organization is unique, and the levels of exposure are different. By conducting a proper risk analysis, the controls or safeguards will address specific needs of the institution.

This article presents a set of recommendations to perform a risk analysis to help *HEIs* and their staff to start an information security strategy in the institution.

This paper is organized as follows. Section II presents the state of the art. Section III presents an explanation of education information systems. Section IV describes the risk analysis functionality. Section V describes the development of this research. Section VI presents the results of this research and Section VII conclusion and future work.

II. STATE OF THE ART

Because *IT* provides opportunities to improve educational services' quality, *HEIs* have increased the use of *IT* to support their processes. Chen [4] mentions that the benefits of *IT* in education environment have attracted researchers attention. The document emphasizes that people, especially in the field of education, often ignore the risk in their processes, assets and *IS*. The risk in the education field should not be ignored and must be considered an important role to promote the development of innovative, protected and managed processes.

On the other hand, Sari [2] states that if an information system within an organization, including *HEIs*, is not safe or well protected, it will be a risk. Lack of control and

 ISBN: 978-1-61208-582-1

prevention of data loss caused by disasters or security incidents, as well as inadequate recovery after disasters, will prevent institutions to continue their business.

Information security should not only be based on technological security tools, but should also be backed up by a good understanding of people in universities, about what processes or assets must be protected, and how to provide the right solution. It means that *HEIs* need a good information security management since they have potential security threats. Also, the document mentions internal and external factors that can influence the implementation of an *Information Security Management System* (*ISM*S) in an organization, which is necessary to protect its information.

An *ISMS* is constructed by some formal and informal controlling process as well as a technique that is applied to overcome any security risk. Its basic form could contain four phases, such as: identifying threats that could attack information sources, defining risks that could result from threats, determining information security policy, and implementing solutions to control and overcome the risk [2].

Furthermore, Azmi [5] states that data leak issues are due to a rapid growth of computer technologies that have resulted in an increase of vulnerabilities in systems. Many institutions, specifically educational institutions, have large amounts of personal data and they need to implement higher levels of security in their systems to stop any attempts of unauthorized users trying to access critical data intentionally. If adequate measures are not considered, records belonging to staff as well as students can be manipulated and used by unauthorized people. Finally, Azmi emphasizes that a risk analysis has to be done to understand the security level of an educational institution.

All of the above references consider implementing security strategies to protect against different risks in processes, assets and information systems of educational institution, but they do not mention how. This paper presents recommendations for performing an easy risk analysis in *HEIs* to identify threats and risk of their information assets.

III. EDUCATION INFORMATION SYSTEMS

HEIs are usually organizations where people receive education, conduct research, exchange knowledge. However, *HEIs* and their affiliated organizations, have a sufficient amount of official, confidential, and restricted data, which must be protected. Loss or disclosure of confidential information could result in property damage, financial and damage to their reputation, among others.

A wide range of processes, assets and information can be protected in *HEIs* such as: customer data, intellectual property, legal and financial records and correspondence.

There are certain areas that are in need of protection, such as [6]:

- Educational and research (tests, examinations, research and development information, intellectual development, information about students, research projects, etc.)
- Human Resources (data on staff and students, personal data, reports, etc.)
- Legal (internal documentation, contracts, confidential information about employees, even after termination of their employment, etc.)
- Financial and economic (procurement documentation, financial information, etc.)
- *IT* (databases, their infrastructure, *IT* management information, logins and passwords, copyright of *IT* developments, etc.).

Information is a critical resource in the operation and management of modern organizations. This is also true for *HEIs*. Availability of relevant information is vital for effective performance of managerial functions such as: planning, organizing, leading, and control. Today, *IS* are the link to connect all the components of organizations and universities and their departments, to provide better operation and survival in a competitive environment.

An education information system is a computer system, which collects, transmits, processes, and stores data within an educational institution, specifically *HEIs*. It is designed to support operations, management, and decision-making functions of the *HEIs*, as shown in Figure 1.

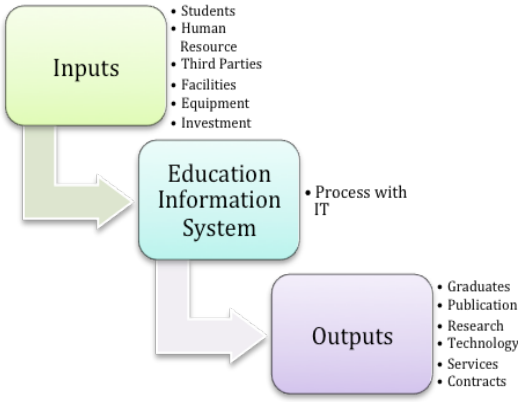

Figure 1. Educational Information System

Because of the growing use of information and its evolving nature, reforms at or within *HEIs* have an increased responsibility to ensure that they have robust policies in place to ensure confidentiality, integrity, and availability of their information. There are different factors that force *HEIs* to develop a security strategy to protect their *IT* assets that support their processes, such as [3]:

- New technologies, like mobile devices, wireless computing, virtual learning environment and portal software, digital libraries, etc. offer new possibilities for teaching, learning and research;
- University authorities, staff and users require a higher quality in their services specifically *IT* knowledge and systems;
- As *IT* and information systems continue to become deeply embedded in many activities and processes of *HEIs*, there is greater need to develop sophisticated models and make initial *IT* investments in infrastructure which would ensure that *IS* are robust and flexible to cope with changing requirements;

 ISBN: 978-1-61208-582-1

- The growing complexity of *IS*, their information technologies and inter-relationships increases difficulty for management to ensure that investments in security controls are aligned to institutional objectives.

IV. RISK ANALYSIS

The objective of risk management is to reduce risk to an acceptable level. An information security risk analysis is a technique to identify and assess threats that may jeopardize an organization's processes and information assets. This technique also helps define security controls to reduce the probability of these threats from occurring.

Risk assessment is the estimate of threats that could exploit vulnerabilities that may cause harm to an asset, resulting in implementation of controls and safeguards to prevent identified risks from ever occurring and recovery plans if a risk becomes a reality in spite of all efforts, this process is known as risk mitigation [7].

The rapid development of *IT* and how to ensure and reduce potential risks of information systems, has been the focus of many organizations and academic areas. Risk assessment is an effective way to solve this problem. However, there are some issues in risk assessment process, such as evaluation indicators, that are difficult to be quantified because risk values are difficult to be defined in *HEIs*.

Once a risk analysis has been conducted, it will be necessary to conduct a risk assessment to determine what threats exist that could avoid achieving institutional mission of *HEIs*. These threats must be prioritized and possible safeguards and controls must be selected. To be effective, a cost-benefit analysis is necessary to determine which controls will help mitigate the risk to an acceptable level for the institution. Another important factor to consider in this process is the impact of regulatory compliance issues.

In conducting the risk assessment, consideration should be given to the advantages and disadvantages of quantitative and qualitative assessments. The main advantage of the qualitative style of risk assessment is that it prioritizes the risks and identifies areas for immediate action and improvement. The disadvantage of qualitative risk assessment is that it does not provide specific quantifiable measurements of the magnitude of the impacts, therefore making a cost-benefit analysis of recommended controls more difficult.

The major advantage of quantitative risk assessment is that it provides an impact magnitude measurement, which can be used in the cost-benefit analysis of recommended controls. The disadvantage is that, depending on the numerical ranges used to express the measurement, the meaning of the quantitative risk assessment may be unclear, requiring the results to be interpreted in a qualitative manner [7].

On the other hand, risk management is an essential part of an *ISMS* that requires measuring and assessing risks as well as reviewing and re-evaluating risks at a later stage to ensure that an effective information security strategy has implemented. Without being well informed about the risks an organization cannot achieve effective security management.

An *ISMS* is a systematic approach to managing sensitive organization information so that it remains secure. It includes people, processes and *IT* systems by applying a risk management process. There are different frameworks to implement an *ISMS* as ISO 27001, which is an international standard. It can help small, medium and large organizations in any sector to keep their information assets secure.

A. Risk Analysis of MAAGTICSI

In Mexico there is a mandatory guidelines for information and the management of communication technologies assets as well as their security, called *MAAGTICSI* (Manual Administrativo de Aplicación General en las materias de Tecnologías de Información y Comunicaciones y de la Seguridad de la Información, Administrative Manual of General Application in Information and Communication Technologies and Information Security). It is aimed at large public agencies and requires many resources for its implementation. *MAAGTICSI* includes a framework to implement an *ISMS* and perform a risk analysis taking reference from international standards and best practices of information security as ISO 27001, ITIL and COBiT.

The framework has a process called Information Security Management (*ASI*, Administración de Seguridad de la Información) that includes a methodology to perform a risk analysis. The objective of this analysis is to identify, classify and prioritize the risks to evaluate its impact on institutional processes and services to obtain risk analysis matrix.

Some activities that *HEIs* could implement to perform a risk analysis to start an information security management are [9]:

1) Establish risk management policy
2) Integrate risk analysis team
3) Identify critical processes
4) Identify information assets and person in charge
5) Identify vulnerabilities
6) Identify threats
7) Conduct identification and evaluation of risk scenarios
8) Develop cost-benefit analysis of security controls

In the case of educational institutions they often do not have sufficient and specialized human resources to carry out all the tasks of an *ISMS* or risk analysis to meet their particular needs, and therefore require other strategies to help them secure the critical assets that support their processes and comply with applicable regulations as *MAAGTICSI*.

V. DEVELOPMENT

The following sentences describe some steps to perform a risk analysis in *HEIs* with some recommendations to help the staff in charge of carrying out the activities according to requirements of the institution.

1) Determine critical processes of *HEIs*. One of the most important activities in risk analysis is to determine critical processes to which the analysis will focus. In *HEIs*,

 ISBN: 978-1-61208-582-1

critical processes are significant processes linked to this type of organization that allow them to achieve their institutional mission.

There are different processes associated with their operation and daily activities of *HEIs*, such as: student enrolment, staff assignment, student assessment, online education, scholarship assignment, research, academic planning, website, financial management, infrastructure management, collaboration agreements, among others.

Recommendation: Senior managers and staff in charge of information security management must establish a procedure to determine critical processes and take into account mainly those that support the institutional mission in the *HEIs*, and identify them with a unique number. For example, Table I shows the identification of a process that belongs to Maestría en Ingeniería en Seguridad y Tecnologías de la Información (*MISTI*) in the Sección de Estudios de Posgrado e Investigación of ESIME Unidad Culhuacan and was assigned a consecutive number as '01'.

TABLE I. PROCESS IDENTIFICATION.

Process Identification ("Process ID")		
[Acronym of Unit or Agency]	***[Area]***	***[Consecutive number]***
SEPICUL	MISTI	01
SEPICUL-MISTI-01		

2) Identify information assets in *HEIs*. Today, most of processes mentioned above have information systems and assets (which are information resources), in their activities e.g., hardware, software, communications, information, facilities and offices, image and reputation, people. It is necessary to establish an ISMS for all of them to guarantee their confidentiality, integrity and availability.

Some assets related to processes in *HEIs* are shown in Table II:

TABLE II. ASSETS IN HEIS.

Assets in HEIs		
Facilities	File servers	Personal records of employees and students
Administrative offices	Websites	Electronic files
Laboratories	Databases	Physical files
Site	Developed computer applications	Email accounts
Network infrastructure	Desktop computers	Research
Web servers	Personal computers	Collaboration agreements
Database servers	Specialized equipment	Contracts
Mail servers	Report cards	Financial statements

Recommendation: Once the assets belonging to critical processes have been identified, it is necessary to assign them an identifier, also describing them briefly, as well as register their managers, then, if it is possible to know their criticality within one or several processes in the institution to continue with the risk analysis, as is shown in Figure 2.

Process ID	Asset ID	Information Asset	Description	Clasification (critical/non-critical)	Responsible public servant
SEPICUL-MISTI-01	MISTI1-001	Site	Place where storage and services servers, and network devices are hosted	Critical	Network Administrator

Figure 2. Asset register

3) Establish an objective and scope of risk analysis.

Recommendation: It is recommended to propose an objective and scope taking into account critical process and information assets, and resources available to perform activities (human, material and time).

For example:

- Objective: To make necessary calculations to establish relative value of risk for each scenario, according to activities of the selected risk analysis methodology.
- Scope: The scope of evaluation is to establish risk values for risk scenarios associated with information assets of *MISTI* critical processes.

4) Make a list of possible threat scenarios in *HEIs* taking into account provided scenarios by *MAAGTICSI* and selecting only those that could apply to the scope and size of *HEIs*.

Recommendation: Reviewing the environment of *HEIs* to select threats and threat agents that may affect them, some examples, as shown in Figure 3.

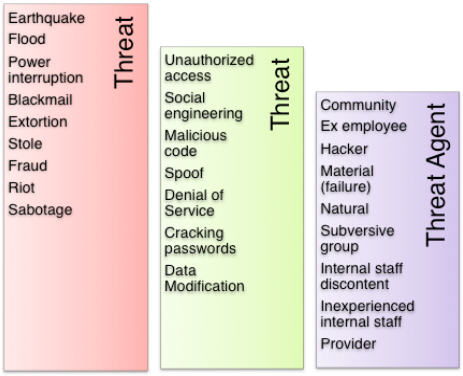

Figure 3. Threat scenarios

An example of a threat scenario is shown in Table III, which was assigned an identifier to recognize it during the process.

TABLE III. THREAT SCENARIO

Threat ID	**Threat**	**Threat Agent**
1032	Denial of service	Discontented internal staff (intentional)

5) Choose one of two suggested procedures to assess risk scenarios:

 ISBN: 978-1-61208-582-1

a) Use traditional method with high, medium and low scale to determine probability of occurrence of a threat and impact to institution to assess risk.

b) Apply a more objective evaluation method to determine the value of probability and impact. For probability additional factors associated to five different scales with representative values from 0.1 to 0.9 are included, as:

- Existence of threat agent from the perspective of a particular information asset (exist)
- Interest of threat agent to attack information asset (want)
- Ability of threat agent to attack the information asset (can), and
- Vulnerability of information asset

The impact considers aspects as: human, material, financial, operational and image with five scales also with representative values from 2 to 10.

Recommendation: If *HEIs* have few resources it is recommended to apply first method. The second method is recommended for staff with experience to facilitate the evaluation, as it becomes a complicated procedure.

6) Choose a form of risk treatment: avoid, prevent, mitigate, finance or assume threat scenarios.

Once the risk value of each threat scenario for each evaluated information asset is obtained, *MAAGTICSI* orders that all threat scenarios with a risk greater than 1.8 should be treated, a situation that for many institutions, especially *HEIs*, it will not be possible to accomplish when implementation of an information security strategy is in its initial stage and has generally limited resources.

Recommendation: In order to compensate for this issue, it is proposed to use another strategy that, instead of being based on threat scenarios, obtains an average risk value of information asset that allows it to know its risk level and considers a minimum risk value of 6 to set priorities for the care of information assets.

The risk matrix proposed by *MAAGTICSI*, shown in Figure 4, can be taken as a reference to indicate the risk value of assets.

Probability of de Ocurrence						
0.9	Almost sure	1.8	3.6	6.4	7.2	9
0.7	High	1.4	2.8	4.2	5.6	7
0.5	Medium	1	2	3	4	5
0.3	Low	0.6	1.2	1.8	2.4	3
0.1	Almost impossible	0.2	0.4	0.6	0.8	1
		Insignificant	Significant	Serious	Critical	Disastrous
		2	4	6	8	10
		IMPACT				

Figure 4. Risk Matrix (MAAGTICSI)

7) Perform a cost-benefit analysis, since not all risk scenarios will be possible to attend immediately.

Recommendation: It is proposed to use another representation form to help this task. For example, the risk matrix presented in Figure 5, which helps to make a decision when reflecting risk level of information assets and their required attention level.

8) Select security controls that will be applied to most critical information assets in *HEIs* to reduce their risk level.

Recommendation: The staff may take as base reference list of security controls in Annex A of ISO 27001.

.

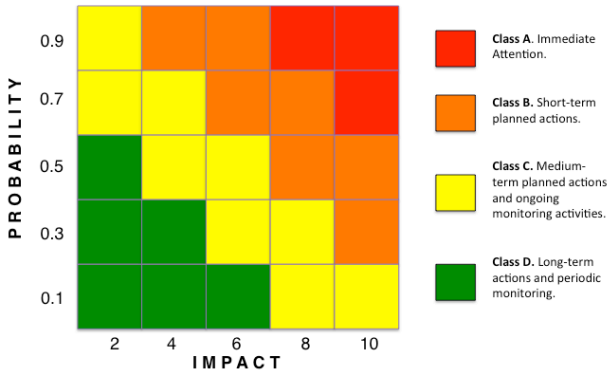

Figure 5. Proposed Risk Analysis Matrix

The general description made above shows some steps that information security management staff may perform a risk analysis in *HEIs*, to know their risk level of their information assets that support their critical processes.

VI. RESULTS

After following risk analysis procedure, steps and recommendations presented and applied to an HEI. The cost-benefit analysis was easy to perform with help of proposed risk matrix, as shown in Figure 6.

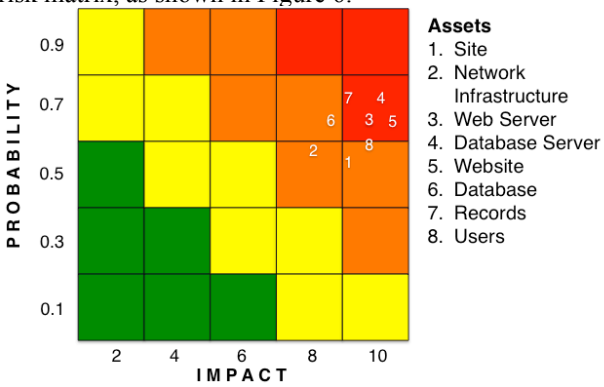

Figure 6. Result Risk Analysis Matrix

The previous matrix allowed us to make better decisions to determine risk treatment and to appropriately select safety controls to be applied when recognizing critical assets of HEI. For example, in this case, the assets that need to be attended to immediately are database server records, website and web server.

VII. CONCLUSION AND FUTURE WORK

With the shown recommendations, *HEIs* may perform an easy procedure to their risk analysis based on *MAAGTICSI* that could help them start generating a security strategy to protect their processes, information assets and data that manage through *IS* and *IT*, as well as, reduce the risk level by security controls selection to attend timely needs of the institution according its special requirements.

 ISBN: 978-1-61208-582-1

As future work, we propose to develop a framework to establish *ISMS* for *HEIs* and analyse institutions of other educational levels with procedures and recommendations presented.

ACKNOWLEDGMENT

We thank the Instituto Politécnico Nacional for the support granted during the development of this research.

REFERENCES

[1] OAS y Symantec Corporation, "Cyber Security Latin America and Caribbean Report," Organization of American States and Symantec Corporation, Multidimensional Security Organization of American States and Government Affairs and Global Cybersecurity Policies, 2014.

[2] P. K. Sari, N. Nurshabrina, and Candiwan, "Factor analysis on information security management in higher education institutions," *2016 4th International Conference on Cyber and IT Service Management*, Bandung, 2016, pp. 1-5.

[3] A. Adamov, M. Erguvan, and D. Ş. Durmaz, "Towards good governance through implementation of University Management Information System: Qafqaz university's Experience," *2010 4th International Conference on Application of Information and Communication Technologies*, Tashkent, 2010, pp. 1-7.

[4] Y. Chen, "Risk management of education information," *2011 IEEE International Symposium on IT in Medicine and Education*, Cuangzhou, 2011, pp. 170-173.

[5] I. M. A. G. Azmi, Q. M. Ashraf, S. Zulhuda, and M. B. Daud, "Critical data leak analysis in educational environment," *2016 4th International Conference on Cyber and IT Service Management*, Bandung, 2016, pp. 1-6.

[6] A. Boranbayev, M. Mazhitov, and Z. Kakhanov, "Implementation of Security Systems for Prevention of Loss of Information at Organizations of Higher Education," *2015 12th International Conference on Information Technology - New Generations*, Las Vegas, NV, 2015, pp. 802-804.

[7] T. R. Peltier, "Information Risk Analysis," (2ª ed.), USA: Auerbach Publications, 2005.

[8] Á. Gómez Vieites, and C. Suárez Rey, "Information Systems - Practical tools for business management," (4ª ed.), México: Alfaomega, 2012.

[9] Secretariat of Public Function, "Administrative Manual of General Application in Information and Communication Technologies and Information Security," Secretariat of Public Function. México: Official Journal of the Federation, 2014.

 ISBN: 978-1-61208-582-1