ORGANIZATION INFORMATION SECURITY RISK MANAGEMENT STRATEGY

Col. Dr. Eng. Iulian N. Bujoreanu, Ph.D., M.A.

Departamentul Regional de Studii pentru Managementul Resurselor de Apărare

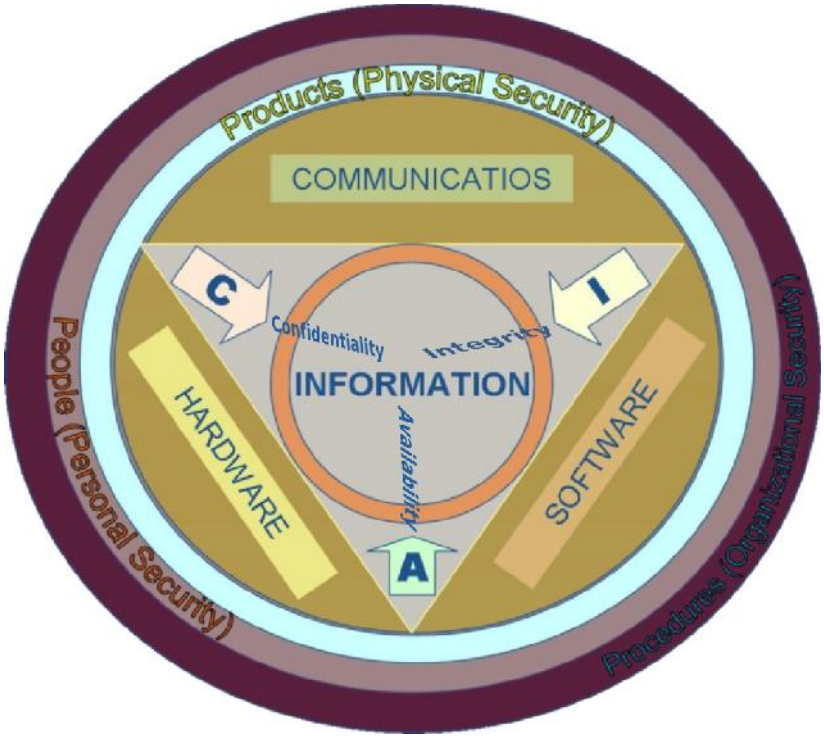
Abstract

Through analyzing the components of the information protection domain, the paper details the steps risk analysis and risk management for this category of activities. Furthermore, it aims to create an organizational framework and practical application of the principles of risk management and analysis through a new approach for the Regional Department of Defense Resources Management Studies with direct intention to deepen the protection of information within the organization.

Introduction

Information Systems are decomposed in three main portions, hardware, software and communications with the purpose to identify and apply information security industry standards, as mechanisms of protection and prevention, at three levels or layers: physical, personal and organizational (see figure bellow[1]). Essentially, for the purpose of information security, procedures or policies are implemented to tell people (administrators, users and operators) how to use products to ensure information security within the organizations.

[1] http://en.wikipedia.org/wiki/Image:Information_security_components_JMK.png



Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms.

Governments, military, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their employees, customers, products, research, and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers. Should confidential information about a businesses customers or finances or new product line fall into the hands of a competitor, such a breach of security could lead to lost business, law suits or even bankruptcy of the business. For governments or military would be even worse by letting them in the hands of any criminal organization, adversary or individual. Protecting confidential information is an organizational requirement, and in many cases also an ethical and legal requirement. For the individual, information security has a significant effect on privacy, which is viewed very

differently in different cultures. It offers many areas for research and development, including Information Systems Auditing, Business Continuity Planning and Digital Forensics Science, to name a few.[2]

After the implementation of the information security policies, practices, measures and applications, everything is supposed to run smoothly. Still, there are risks challenging and affecting further the organization's activities for they were not taken into account initially when the information security framework was designed. Here come the risk management activities to fill the gap.

Security is everyone's responsibility. The CISA Review Manual 2006 provides the following definition of risk management: "Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving organization objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization."[3]

The *process* of risk management is an ongoing iterative process. It must be repeated indefinitely. The organization environment is constantly changing and new threats and vulnerabilities emerge every day. The choice of countermeasures (controls) used to manage risks must strike a balance between productivity, cost, effectiveness of the countermeasure, and the value of the informational asset being protected.

The deployment of a risk management framework for information security brings the dynamic aspects under control, as long as the organization is still viable. It can also bring the necessary improvements to the information security framework in order to avoid further influence over the organization's activities from the currently treated risks.

The likelihood that a threat (anything - man made or act of nature - that has the potential to cause harm) will use a vulnerability (a weakness that could

[2] http://en.wikipedia.org/wiki/Information_security
[3] http://www.isaca.org/

be used to endanger or cause harm to an informational asset) to cause harm creates a risk (the loss of an asset). When a threat becomes active, it has an impact. In the context of information security, the impact is a loss of availability, integrity, and confidentiality, and possibly other losses (lost income, loss of life, loss of real property). It is not possible to identify all risks, nor is it possible to eliminate all risks. The remaining risk is called residual risk.

Organization Description

For the organization personnel, risk taking represents a hard option among other options they might have to take. Generally, an organization exhibits aversion to risk in a high degree in order to protect itself from losing assets or resources. My organization is an educational institution and, for the reason of being as open as possible, it does not show excessive aversion to risks. This is because the personnel (especially the teaching staff) have to get in touch with so many other people that are not directly belonging to the organization. As a result, by assuming some higher level of risk in opening so much the organization's level of access to different sources (databases, books, and other references) one can see that there is a need for a better understanding of risk management in information security providing for the proper functioning of the organization.

A risk assessment should be carried out by a team of people who have knowledge of specific areas of the business. Membership of the team may vary over time as different parts of the organizational processes are assessed. The assessment may use a subjective qualitative analysis based on informed opinion, or where reliable financial figures and historical information is available, the analysis may use quantitative analysis.

The ISO/IEC 27002:2005 (an information security standard published by the International Organization for Standardization and the International Electrotechnical Commission as ISO/IEC 17799:2005 and subsequently

renumbered ISO/IEC 27002:2005 in July 2007) Code of practice for information security management recommends the following be examined during a risk assessment: security policy, organization of information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, information systems acquisition, development and maintenance, information security incident management, business continuity management, and regulatory compliance.

In broad terms the risk management process consists of:

1. Identification of assets and estimating their value. Include: people, buildings, hardware, software, data (electronic, print, and other), and supplies.

2. Conduct a threat assessment. Include: Acts of nature, acts of war, accidents, and malicious acts originating from inside or outside the organization.

3. Conduct a vulnerability assessment, and, for each vulnerability calculate the probability that it will be exploited. Evaluate policies, procedures, standards, training, physical security, quality control, technical security.

4. Calculate the impact that each threat would have on each asset. Use qualitative analysis or quantitative analysis.

5. Identify, select and implement appropriate controls. Provide a proportional response. Consider productivity, cost effectiveness, and value of the asset.

6. Evaluate the effectiveness of the control measures. Ensure the controls provide the required cost effective protection without discernable loss of productivity.

For any given risk, organization leadership can choose to *accept the risk* based upon the relative low value of the asset, the relative low frequency of occurrence, and the relative low impact on the organization activity. Or, leadership may choose to *mitigate the risk* by selecting and implementing appropriate control measures to reduce the risk. In some cases, the *risk can be*

transferred to another organization by buying insurance or out-sourcing to another organization. The reality of some risks may be disputed. In such cases leadership may choose to *deny the risk*. This is itself a potential risk.

Current Risk Management Approach

Currently, my organization applies risk management in a traditional fashion. It is based on rules and regulations, there is no specific plan or strategy for applying a scientific approach in managing the risks, and it takes no more than five minutes for the person in charge to shut down the network, in case some risks might be sensed, to avoid further losses.

The need to develop deeper and more detailed plans to take into consideration the management of the risks the network might be facing was not that strong for several reasons. First of them was the very main mission of the organization that was education. As in any educational organization, it is expected to have a higher degree of "freedom" that, compulsory attracts higher risks against a smoother running of the organization network. In reality, the computers of the network that belong to the students have a standard configuration that allows for a very thin layer of protection. Besides that protection, there is nothing but the reinstalling of the operating system or of the image of the partition containing the operating system together with the main software programs a student might be interested in using during his/her staying in the organization.

Second reason was the lack of knowledge in the field of information security, both for the leadership and other personnel in the organization. For this reason, the IT team has never insisted, but very little, in getting to a strong point in providing information security. This, again, let them no other choice than acting dramatically with respect to any workstation by reinstalling the operating system as new (this is not a choice when some valuable documents, papers,

references have been gathered, in time, and the user would very much prefer to keep them, instead of looking for them again).

Another reason would be the lack of interest of the personnel to let the network function as it should be. There were a series of incidents with different computers that have shown that, in different situations, applying or using tools, instruments or practices that are not according to the internal regulations (on which they have been instructed but they do not respect) the impact of that assumed risk was greater than it was thought of (although the loss was database or time fro different classes or applications and the professors have had their own backup for that).

One section of the network is the only one that has a greater attention from the leadership and this is because it represents the group of workstations that are used by the command officers to coordinate the organization functioning. This is used to convey internal documents, not open to the public or to the students. The risk management for that one has been solved easily, by cutting any connection between that side and the rest of the network (again, the easiest possible measure that does not take into account a possible extension that would make harder the operation in an isolated environment).

Essential Elements of an Information Security Risk Management Program

If one takes into account the size and importance of my organization, a risk management program in my organization should be both comprehensive and easily applicable because of the reduce number of personnel capable to develop activities in this area.

It will identify and document the components of the risk management program, including roles and responsibilities, processes, and measures of success.

The structural processes that are to be controlled in the new risk management strategy will be: leadership (command, control and communication connections), administration (connection within the administrative elements of the organization – financial, logistical, material, etc. and between these and other elements, both internal and external), and education (with both teaching staff and library, and students sides of the network).

In order to plan and work for the implementation of the information security risk management program, a team will be appointed to work on this issue. Whole team will not have more than three members. I will lead the team to ensure both impartiality (by not being a member of the IT team) and knowledge of how to lead the process on. Other members will be the deputy commandant, the head of the IT office, and the head of the secretariat office that has to supervise the correct implementation of the regulations in the organization activities. The counterintelligence officer, not being directly part of our organization will be consulted in different critical moments of our activity.

Each member of the team and the team together will gather information that is necessary to cover each of the stages included in the risk management process. Finally, the team will come out with a draft strategy for the risk management of the information security in the organization that will be submitted for approval.

The activities and documents to be developed will follow the algorithm of the risk management process build-up:

1. Identification of assets and estimating their value. Include: people, buildings, hardware, software, data (electronic, print, and other), and supplies.

This is going to be assigned to the deputy commandant and IT office. First, they will come with a list of people involved in different activities with assigned priorities of security on them. Because of the reduced personnel, there is enough “room” to analyze each person and address any security risk that person might bring. Generally, the personnel categories will have some security

levels assigned so that they differentiate among themselves with respect to different levels of access over the entire network. Highest level of access will be granted to the commandant and the leadership team.

Similarly, there will be a document containing the list of buildings, offices, access entries, destination for each room. It will be presented the current use for each room and the possible change, if necessary, in the case a better achievement or coverage for risk avoiding or mitigating on some tasks would be possible.

Finally, for this chapter, the lists with existing hardware, software, databases (electronic, print, and other), and supplies should be detailed enough in order to provide the understanding of other sources of risk factors one has to additionally take into account.

2. Conduct a threat assessment. Include: Acts of nature, acts of war, accidents, and malicious acts originating from inside or outside the organization.

Next step, after getting the complete image of the organization with everything it has in it, is to analyze each of the elements in the lists previously mentioned and assess what threats can come out of any of those. The team for the risk management process will interact with each member of the organization for both acknowledging the existence of some risk factors and identifying the possible ways to cope with that risk factor. For acts of nature or of war, or accidents there is a clearly understood set of procedures that, in as short of a timeframe as possible will bring the organization back in operation. It involves spare rooms for the servers, spare parts for the workstations and other network components, repairing, replacing, removing and reconnecting elements of the network. As far as malicious acts are concerned, both inside and outside actors should be analyzed. The outside actors are specifically those related to the students that come for different courses provided by the organization, and try, using different methods to penetrate into network areas they are not allowed to.

3. Conduct a vulnerability assessment, and, for each of the vulnerabilities, calculate the probability that it will be exploited. Evaluate policies, procedures, standards, training, physical security, quality control, technical security.

After understanding under what sort of threats the organization is supposed to operate, there will be a deeper analysis of the vulnerabilities that might be exploited under different scenarios by the risk factors enumerated above. For example, there will be a different approach on students accessing the network from there apartments, and their accessing the network from the classrooms or the professors' offices. A compulsory scanning procedure will be set for any device used to input data into any work station, in the teaching rooms. That will provide, later, an easier access to any resource one might need to access. It will be easier for the teaching staff. The students will have a different level of access and this is where, via access control and filtering, the main part of the information security risk management is to be provided. A bit more difficult will be to impose the teaching staff the same procedures but, any change comes with sacrifices and everybody has to understand that the change is for their own good.

4. Calculate the impact that each threat would have on each asset. Use qualitative analysis or quantitative analysis.

Using the qualitative analysis, because there is no quantitative data on level of impacts the threats have had on the organization network, the team will develop a calculation on what the impact means. It will be converted in work-time for the IT people, lost time for education during classes, lack of access to the internet and slowing down the pace of solving tasks for anybody in the organization (jobs for leadership and administration, assignments for students, etc.). As an example, for each situation when there is no access for the teaching staff to use a simple flash memory stick in order to bring a new case or problem to the students, beside those existing in our databases already, the effective time

for teaching will be reduced by at least ten minutes, that is the time needed to solve the new problem that was supposed to be presented. In this case, one can qualitatively assess that such a perturbation can stop the trend of improving the teaching process. In this case, excuses are nice but ineffective for the overall activity of the organization.

5. Identify, select and implement appropriate controls. Provide a proportional response. Consider productivity, cost effectiveness, and value of the asset.

Following the analysis of the impacts each threat should have on the organization general status, the risk management team will work to identify the necessary controls that allow for a good development of the entire activity. As far as the leadership is concerned, there will not be any opposition with regards to implementing more security measures. There is a general agreement for implementation of security measures; it only has to be reanalyzed in what it means implementing a security control. The controls will be grouped in access controls (for users, both inside and outside the organization, for different types of access), data (and databases) protection (including regular backups), and physical protection (for the workstations and the rooms where IT can be found). The most important assets to be protected and controlled are those belonging to the classified network. There is no cost effectiveness for that (actually the cost is so high that it is useless to speak about costs – the entire organization is to be affected in a totally negative way). The workstations and databases used by the teaching staff come next. The entire education process can be stopped or at least delayed by destroying a database with applications and problems. The elements of the network operated by administrative staff follow and the student workstations are last priority because they are the most numerous and easily to be replaced or reset.

6. Evaluate the effectiveness of the control measures. Ensure the controls provide the required cost effective protection without discernable loss of productivity.

In this final stage there will be an analysis development that will make the process repetitive for as long as it needs to adjust the network reaction following the new security measures implementation. There will also be set a periodic revisiting of the risk management framework for information security that is to be implemented.

A number of activities swill be recorded and the effectiveness of the security measures implementation is to be calculated. It means, for example that I will quantify each break in the teaching time that appears following the lack of access to the network of a professor (coefficient 3), student (coefficient 2), other own officer (coefficient 5 for leadership, 4 for administration), or other visitor officer (short time visits, coefficient 1). This coefficient will model the effectiveness of the security measures by adjusting the formula for effectiveness provided bellow:

$$\text{Effectiveness} = \Sigma\ [(\text{No. of interventions} / \text{Total time of operation}) \times \text{Coeff. of importance}]$$

$$\text{Security provided} = \Sigma\ [(\text{No. of interventions} / \text{Time out of operation}) \times \text{Coeff. of importance}]$$

There will be set a table of conversion for any type of activity that is to be developed following a intervention to fix any damage of a successful threat acting against any of the vulnerabilities.

In the case there appear new vulnerabilities, the measures to adapt the entire set of procedures will be implemented immediately.

The Information Security Risk Management Strategy, as developed by the appointed risk management team, will be finalized and submitted to the commandant in an analysis session so that any question can be answered with the appropriate details and proving materials.

The data for statistics will be continuously gathered and processed so that anyone interested (and in right to question) can see and be explained the course of facts and action required to be taken.

There will also be a periodic information activity for both the leadership and the organization personnel in order to present the evolution and progress made with respect to the implementation of the information security risk management strategy. This way, another goal of the information security will be fulfilled: educating a training of the personnel in the information security field. Awareness measures will be present always, from the access moment until the exiting time.

The senior management of the organization will be explained the reasons for the implementation of a more formal and rigorous framework in providing information security risk management. These would approach the probable extending of the organization structure, personnel, together with the continuous variation of the number of students on a regular basis.

The general concept to be introduced to the senior leadership will be the understanding that, after implementing a certain framework, it will be easier to quantify, assess, and evaluate the general status of the organization with respect to the information security protection it provides, and the way it manages the affecting risk factors (accept, mitigate, transfer, or deny the risk).

It will also bring to the knowledge of the leadership the possible alternatives. I would propose to implement the strategy as it is, without any diminishing argument. This way, that is also feasible, will let the organization with a better cover for any type of risks. Any other option can be implemented but it means accepting, *a priori* risks that might be avoided otherwise. There

will be an alternative that involves fewer personnel directly involved in supervising the risk management measures. Still, it will be like an extreme option compared to the first to be proposed. This is because the initial alternative has a limited number of acting members that cannot be replaced without giving up some effectiveness inside the team.

The strategic perspective for senior management is to understand the future increasing information security needs based on the perspectives offered by the educational dynamics in the future course offered by the organization, other international activities and seminars that will take the interest for this strategy to a higher level based on the quality of the participants in the communication processes that will be developed on different occasions.

REFERENCES

Gary Stoneburner, Alice Goguen, and Alexis Feringa (2002), *Risk Management Guide for Information Technology Systems*, NIST Special Publication 800-30.

Stamp, Mark.(2006), *Information security: principles and practice*, JohnWiley & Sons, Inc., Hoboken, New Jersey.

Jim Gunther, *101 Rules of Risk Management*, Harvard Aimes Group, http://www.riskmanagementsearch.com/rules.asp.

Jeevan Jaisingh and Jackie Rees, *Value at Risk: A methodology for Information Security Risk Assessment*, Krannert Graduate School of Management, Purdue University, West Lafayette, IN.

John Shortreed, John Hicks, Lorraine Craig (2003), *Basic Frameworks for Risk Management-Final Report*, Network *for* Environmental Risk Assessment *and* Management, The Ontario Ministry of the Environment, Canada.

Khalid Kark (2007), *Building information risk management frameworks: Developing controls for people, processes and technology*, RISK MANAGEMENT STRATEGIES, http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1265294,00.html.

Dr. Ron Ross (2006), *Building More Secure Information Systems*, A Strategy for Effectively Applying the Provisions of FISMA, Gaithersburg, MD USA 20899-8930.

Brian Denis Egan (2005), *Decision Analysis and Risk Management: Two Sides of the Same Coin*, Expert Reference Series of White Papers, Global Knowledge Network, www.globalknowledge.com.

Virchow Krause (2005), *Enterprise Risk Management: The Road to Implementation*, www.VKutilities.com.

Virchow Krause (2005), *The Principles of Enterprise Risk Management*, www.VKutilities.com.

Brian W. Nocco and René M. Stulz (2006), *Enterprise Risk Management: Theory and Practice*, Ohio
State University.
Julia H. Allen (2006), *How Much Security Is Enough*, Carnegie Mellon University, https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/management/566.html.
Information Risk Management (2008), RSA Security Inc. www.RSA.com, www.EMC.com and http://www.in.kpmg.com/services/services_irm.asp.
Randy Wheeler (2005), *Seven Principles of Risk Management*, The John Liner Review, Vol. 18 No. 4
Winter 2005.
George Wang (2005), *Strategies and Influence for Information Security*, Information Systems Control Journal, Volume 1, 2005, http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=34579&TEMPLATE=/ContentManagement/ContentDisplay.cfm.
Jay G Heiser (2004), *The regulation of information security*, International Institute of Communications, Intermedia, London: July 2004. Vol. 32, Iss. 2; pg. 29.
Stephen Rogers, Robert Torok, and Stephen (2007), *Thinking Through Uncertainty*, A report prepared by CFO Research Services in collaboration with IBM Corporation, CFO Publishing Corp.
Joan T. Schaming (1997), *What Is This Thing Called Risk Management*, Survive! Magazine, http://www.disaster-resource.com/cgi-bin/article_search.cgi?id='60'.