ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

CESIA | CENTRO SERVIZI INFORMATICI DI ATENEO

Feedback by the University of Bologna on Risk Profile Classification and Organizational Control Card Selection in the application of OCTAVE method for the Academic environment

Index

1. Introduction

The University of Bologna is one of the important academy institute in Italy with a large number of students, scientific/cultural activities and with a lot of relationships with industries and companies that confirm the relevant role that the university has reached in the last century. Today Bologna is proud to guess an academy institute with a high-specialized administrative/technical staff for offering quality services to academy's best customers: the students.

The most important roles is play by Center for the Management and Development of Services (CESIA) that is responsible for the most important service as: (a) the academic network connection to Internet, (b) the official email service @unibo.it, (c) the hosting of the academic portal web site, (d) development and hosting of dozen of software applications for the administrative areas.

In the last two years another hot topic is faced by the technical staff: How to improve, or create, the security process regarding people, systems and information?

But if CESIA wants to face this challenge it's important to give the dimensions of the problem: 90.000 active students, 12000 administrative/technical/research staff, 90 departments and 20 faculties; and what about the incidents: in 2007 first quarter about 200000 events categorized as high risk by Intrusion Detection System, and in 2007 second quarter about 600000 events categorized as high risk; and in case of compromised host the incident is caused by: the 40% of host is victim of botnet IRC, the 30% of host have no kind of protection as personal firewall or antivirus (if there is one, maybe is not updated) and the remaining 30% has an operative system with no updates and hotfix.

The way used by CESIA to face security for whole academy can be separated in two ordered and distinctive levels: reactive e proactive.

The reactive part is built principally of a brand new group in CESIA called Security Team that constitutes the Computer Emergency Response Team (AlmaCERT). AlmaCERT is responsible for management of intrusion detection system and alarms deriving from it, forward alarm to departments and faculties, manage incidents in collaboration with national/international security teams, implement and deliver proactive service as centralized antivirus platform (based on a commercial software), and centralized windows update system for updating clients and servers.

The proactive part is built on a project called "Risk assessment and management in academy's structure" and is based on the ENISA deliverable "Information Package for

SMEs". The ENISA document on the Risk assessment and management for SMEs should be adapted in case of academy environment.

CESIA and the University of Bologna will provide for ENISA the possibility to extend organizational control cards and asset control cards in an academic network. The main challenge is represented by the fact that in an academic network it is rather unlikely to find equity between research activities (and its natural attitude to experiments and loss of rules and limits) and information security (that is based on the assumption of limitation imposed to use of technological assets and treatment of data and information).

The first objective is to enhance the security level of departments thanks to a standard methodology provided by ENISA. In fact, the "Information package for SMEs" contains a risk assessment/risk management methodology which can be used in case of small, medium and big departments (all of them can be treated as a SME),

The second objective is to focus on a risk profile evaluation table. CESIA wants to give ENISA a feedback in order to rewrite this table when the SME objective of risk assessment project is a PA department. As a matter of fact, "legal and regulatory", "productivity", "financial stability", and "Reputation and loss of customer confidence" and their definitions for a classification in high, medium and low classes are not so appropriate in case of a PA. For example "financial stability" for an almost useless department since its budget depends on general administration of University of Bologna. CESIA wants to rewrite this table, changing the risk areas ("legal and regulatory", "productivity", "financial stability", and "Reputation and loss of customer confidence") and the definition for classifications. Of course, CESIA wants to give indications and suggestions on the appropriate organizational control card selection.

2. Methodology related issues

This chapter will discuss any single aspect emerged in the application of ENISA deliverable "Information Package for SMEs" to departments of University of Bologna.

2.1. Decision makers and outsourcing

Who are the decision makers? In this project are the department's councils and their directors. These staffs are well informed on any single phase regarding risk analysis and risk assessment project, and they have to approve changes from the analysis phase to the implementation of security measures.

The working staff model is based on partial outsourcing and it assumes that the initial risk assessment is provided by CESIA (that is responsible for the whole academic IT network infrastructure), that acts as an external company from the departments point of view. Also, the initial assessment provides knowledge transfer to the department internal personnel. Finally, the implementation phase is performed by CESIA in collaboration with local technicians.

2.2. Risk profile selection

2.2.1. Statement of application

The main problem faced is related to the risk areas in the table of risk profile selection due to the different economical and organizational nature of a department with respect to a SME.

These are the main considerations on risk profile selection:

- The first and the last risk areas, **Legal and Regulatory** and **Reputation and loss of customer confidence** can be easily used for a department. In fact, a department usually manages personal and medical data for research activities. If customers' role is substituted by students is easy to understand why a department has to maintain a correct level of reputation.
- The second and the third risk areas, **Financial Stability** and **Productivity**, have to be modified. A department's financial stability depends on the economic stability of the whole university and, of course, it is more stable than a SME. Departments' productivity can be split in two main areas because a department can be viewed as a very specific SME dedicated to teaching and research.

- If it is not possible to establish the correct profile risk, it is also impossible to use the organizational control cards selection table. This kind of selection is very important to establish a security treatment for the whole organization. The paragraph below shows the right connection between the new risk areas and the organizational control card provided by OCTAVE

2.2.2. Modifications proposed

The main change is dedicated to risk selection where "Financial Stability" and "Productivity" are replaced by:

- **Teaching**: this is the main common and important activity of departments. The risk is high if the unavailability of one of the above services can stop one of the teaching activities and/or if it can cause the loss of data and information related to examinations or student's careers,
- **Research**: this area has a strategic role for many departments and especially for those that are based on their academic prestige on the quality of their research. The research can be classified as a high area risk if the unavailability or the incorrect management of this area (for example, unavailability of laboratories and devices, lack of international relationship, lack of knowledge about fundraising) can have a direct impact on this strategic activity.
- **Patents**: research activities can produce a very specific technological knowledge and, sometimes, these activities can be registered as patents. Patents can lead to economic benefits to support research, international academic prestige and/or collaboration with companies.

The table below shows the modification to table 2 about the ENISA's deliverable "Information package for SMEs" (paragraph 4.3.1, Phase 1 – Risk Profile Selection pp. 20).

Area Risk	High	Medium	Low
Legal	The organization handles customer information of a sensitive and personal nature including medical records and critical personal data as defined by the EU Data Protection Law.	The organization handles customer information of a personal but not sensitive nature as defined by the EU Data Protection Law.	The organization does not handle personal data other than those of the people employed by the organization.
Teaching	**Unavailability or Service Quality directly impact the teaching activity of department (laboratories, libraries, technological classrooms, reservation of classrooms, reservation of**	**Unavailability or Service Quality can indirectly impact on teaching activity of department**	**Unavailability or Service Quality have no impact on teaching activity of department**

	examinations, registration of examinations, students activity)		
Research	**Unavailability or Service Quality directly impact on research activity (laboratories, IT classrooms, libraries, fund raising, international relationship)**	**Unavailability or Service Quality can indirectly impact on research activity**	**Unavailability or Service Quality have no impact on research activity**
Patents	**An infringement of patents will cause the loss of economical benefits and th loss of technological knowledge with respect to competition**	**An infringement of patents may cause the loss of economical benefits**	**the department has no registered patents**
Reputation	Unavailability or Service Quality directly impact the businesses of the organization or/and more than 70% of customer base has online access to business products and services.	Unavailability or Service Quality can indirectly impact the businesses of the organization and/or less than 5% of customer base has online access to business products and services.	Unavailability or Service Quality cannot directly or indirectly impact the businesses of the organization or result in loss of revenues.

Table 1: Risk profile selection

2.3. Critical asset identification

2.3.1. Statement of application

The asset identification remain unchanged because the definitions relating to systems, network, people and applications are suitable also in the case of departments. Only a modification to the examples of assets related to people and applications was required.

2.3.2. Modifications proposed

There are modifications proposed to people and application categories in order to be compliant with typical roles and software application used in a department:

Asset	Description	Asset type
System	Information systems processing and storing information. Systems are a combination of information, software, and hardware assets. Any host, client, server, or network can be considered as a system. Critical systems are those identified as essential for the continuous provision of the business service and product offerings; those that store critical business information (customer or business proprietary) or those that are exposed to the outside world for business functions or services.	Server
		Laptop PC
		Workstation
		Archiving and Backup
		Storage

Network	Devices important to the organization's networks. Routers, switches, and modems are all examples of this class of components. Wireless components/devices, such as cell phones and wireless access points that staff members use to access information (for example, email). Typically, critical networks are those that are used to support essential critical applications or systems or those that are shared with a third party and usually untrusted networks	Routers
		Cabling
		Gateways
		Wireless Access Points
		Network Segment (e.g. cabling and equipment between two computers)
		Firewall
		VoIP
People	People in the organization, including their skills, training, knowledge, and experience. Critical people are those that play a key role in production or operational processes.	**Administrative**
		Technical
		Professor
		Researcher
		Contractors
Application	Critical Applications. Applications that are key to or are part of the product and service offerings. The disruption of critical applications typically results in severe hindering or even congestion of the dependent processes.	**Logistics**
		Personnel Management
		Fund management
		Identity Management
		Network Services Management
		Career Management

Table 2: Asset category classification

2.4. Organizational control card selection

This is the second main modification to ENISA's deliverable (paragraph 4.3.3, Phase 3 – Control Cards Selection, section Organizational Control Cards Selection, table 6, pp. 24).

2.4.1. Statement of application

- The organization control card dedicated to security strategies (SP2) is not present in table 3 "organizational control card selection", because CESIA has centralized the security strategies for all departments. In fact, security strategies cannot depend on single departments, and furthermore this avoids that the choices made by departments vary between structures
- The organizational control card dedicated to Security Awareness and Training (SP1) is present everywhere in table 3, since security awareness and training is considered as the most important step in security risks mitigation, and it is supposed that teaching activities can be organized into an appropriate manner
- According to the academic security strategies and policies, it is important that control cards for the protection of workstations (SP4) are activated even if the department risk profile is classified as low

2.4.2. Modifications proposed

These changes cover all areas, both the changes relating to legal and reputational, and the new areas previously introduced (research, teaching and patents).

Risk Area	High	Medium	Low
Legal	**(SP1)** **(SP3)** **(SP4)** **(SP5)**	**(SP1)** **SP3.2, 3.3, 3.4** **SP4.1, 4.2, 4.3, 4.6** **SP5.1, 5.5**	**SP1.1** **SP3.2, 3.4** **SP4.1, 4.6**
Research	**(SP1)** **(SP3)** **(SP4)** **(SP5)** **(SP6)**	**(SP1)** **SP3.1** **(SP4)** **SP5.1, 5.2, 5.5** **(SP6)**	**SP1.1** **SP3.2, 3.4** **SP4.1** **SP5.1**
Teaching	**(SP1)** **(SP4)**	**(SP1)** **(SP4)**	**SP1.1** **SP4.1**
Patents	**(SP1)** **(SP3)** **(SP4)** **(SP5)** **(SP6)**	**(SP1)** **SP3.1, 3.5, 3.6** **SP4.1, 4.2, 4.6** **SP5.1, 5.2, 5.5** **(SP6)**	**SP1.1** **SP4.1**
Reputation	**(SP1)** **(SP6)**	**(SP1)** **(SP6)**	**SP1.1** **SP4.1**

Table 3: Organizational control card selection

2.5. Implementation and Management

The project execution requires a good IT expertise level; usually, these skills are not found in IT departments. That is why CESIA has included a training phase for IT personnel to the project. The aim is that of creating a centralized management of technicians who may be located in a dynamic way through various departments.

2.6. Final considerations

CESIA was responsible of the editing of some parts of the ENISA deliverable in order to make it suitable for the academic departments. In particular, the editing was focused on risk profile selection and organizational control card selection.

All the other parts remained unchanged, such as any single asset control card, any single organizational control card.

From our experience emerged that the ENISA deliverable is good risk assessment and risk analysis base for the academic environment and fitted the University of Bologna needs with just slight modification to risk profile selection and control card selection.

3. Future works

We suppose that the introduction of a scale for classifying the security level of any single department should be a good idea. This scale is designed to create a sort of ranking for departments. The ranking is updated at any periodic verification of the department's risk profile.

The number of risk areas could be updated by increasing the number of departments, or expanding the project to academic structures (for example, specialized master schools, interdepartmental centers, etc) that have different needs with respect to individual departments.

After implementing the project security in a sufficient number of departments, training courses will be activated to increase the level of information security knowledge among technicians.

The security project provides a phase dedicated to collaboration with other Italian and European universities to exchange information on projects similar to those at the University of Bologna.

The part of the asset-based control cards could be modified for a larger adaptability to the case university, but currently this is not a significant change and improvement for the project. It could still emerge only after an enlargement in terms of nature and number of facilities which the university involves.

ANNEX A: Departments involved

The pilot CESIA-ENISA was tested on three categories of departments as follows:

- **Small departments**: this kind of department does not offer advanced services to their users, and it is composed of a number of employees that does not exceed 10 units. Nor has it a research and limited number of students. The main activities of the department are teaching and management of laboratories, museums and/or libraries.
- **Medium departments**: this type of department has a number of employees that does not exceed 50 units. It has few servers and offers a limited number of services. The department carries out its own research and manages a few laboratories and libraries. The teaching activity draws a good number of students who attend constantly departments and lessons.
- **Large departments**: this type of department offers advanced services and has a server farm operated by specialized personnel. The research is very important and allows the registration of some patents. The teaching activity draws a large number of students. The management of libraries and laboratories is delivered by the presence of technical staff that cover specific tasks.

Department A

Organization	Small
Risk Profile	Legal: None Teaching: None Research: None Patents: None Reputation: Medium
Critical Asset	Systems: Integrity Network: Availability People: None Application: None
Organizational Control Card	(SP1) (SP6)
Asset Control Card	CC-2S
Security Team Member	2

Department B

Organization	Small
Risk Profile	Legal: None Teaching: None Research: None Patents: None Reputation: High
Critical Asset	Systems: Availability Network: Integrity People: None Application: Availability
Organizational Control Card	(SP1) (SP6)
Asset Control Card	CC-1S CC-1N CC-1A
Security Team Member	2

Department C

Organization	Medium
Risk Profile	Legal: None Teaching: Medium Research: High Patents: None Reputation: Low
Critical Asset	Systems: Integrity Network: Integrity People: None Application: None
Organizational Control Card	(SP1) (SP3) (SP4) (SP5) (SP6)
Asset Control Card	CC-2S CC-2N
Security Team Member	4

Department D

Organization	Medium
Risk Profile	Legal: None Teaching: Medium Research: High Patents: High Reputation: Medium
Critical Asset	Systems: Integrity Network: Integrity, Availability People: Integrity Application: Confidentiality
Organizational Control Card	(SP1) (SP3) (SP4) (SP5) (SP6)
Asset Control Card	CC-1A CC-1P CC-1S CC-1N
Security Team Member	5

Department E

Organization	Medium
Risk Profile	Legal: None Teaching: Medium Research: Medium Patents: None Reputation: None
Critical Asset	Systems: Integrity Network: None People: None Application: None
Organizational Control Card	(SP1) SP3.1 (SP4) SP5.1, 5.2, 5.5 (SP6)
Asset Control Card	CC-2S
Security Team Member	5

Department F

Organization	Medium
Risk Profile	Legal: None Teaching: Medium Research: Medium Patents: None Reputation: None
Critical Asset	Systems: Integrity Network: Integrity People: None Application: None
Organizational Control Card	(SP1) SP3.1 (SP4) SP5.1, 5.2, 5.5 (SP6)
Asset Control Card	CC-2S CC-2N
Security Team Member	3

Department G

Organization	Large
Risk Profile	Legal: None Teaching: Medium Research: High Patents: None Reputation: None
Critical Asset	Systems: Integrity Network: Integrity, Availability People: None Application: Availability
Organizational Control Card	(SP1) (SP3) (SP4) (SP5) (SP6)
Asset Control Card	CC-1S CC-1N CC-1A
Security Team Member	6