A Case Study of InterAdria; Regarding Security Strategy of a SME

Ariana Kajtazi
A case study of InterAdria; regarding security strategy of a SME

Author: Ariana Kajtazi
Tutor: Anna Wingkvist
Examiner: Birgitta Fagerström Kareld
ABSTRACT

Today, security strategy has a crucial role in society, which does not imply only to large companies, but also and especially to Small Medium Enterprises (SME’s).
The intention of this thesis is to provide instructions and help enterprises that need assistance in applying proper security strategy. This thesis comprises the most crucial areas of security within an enterprise. Its aim is to study more deeply the situation of the current security strategy, of a telecom and a software development enterprise, by which the enterprise can extract enough information to provide a proper system. The purpose is to study, analyze, explore and bring some conclusions with new ideas on how to improve and propose a new security strategy that can fit and that can be appropriate for this enterprise.
Regarding the exploration and research for the enterprise, “fragile assets” are the target to be taken in consideration such as “software”, “databases” and “important data”.
The method which is used in this thesis, is the case study method, which has best suited the purpose of this thesis by covering the logic of design, data collection techniques and data analysis. As a theory the OCTAVE-sm approach was applied. This approach has three phases which each contains its own processes. These processes were followed and used for the evaluation of the current state in one Small Medium Enterprise (SME) called InterAdria. The use of OCTAVE-sm approach in this thesis can be a guide to all other Small Medium Enterprises (SME’s) that struggle with their security strategy same as the enterprise mentioned above. The conclusion was based on the entire data gathering that was done by following the steps of the Octave-sm approach.

Keywords: Security Strategy, Small Medium Enterprises (SME’s).
Acknowledgments

I would like to express my gratitude to some people that helped me and guided me through my work with this thesis.

Anna Wingkvist as a tutor has done a remarkable job guiding and encouraging me throughout the right direction by giving her best.
Birgitta Fagerström Kareld and Jan Aidenmark which stated their opinions and their ideas on how to make improvements to my work
The managers of InterAdria and its software development employees that found time for helping me gather information upon the current state of security strategy in their enterprise.
I would also thank my family and especially my sister Miranda Kajtazi which supported me all the time even in the long distance.
## Content

1 INTRODUCTION ........................................................................................................................................... 1
   1.1 Problem Definition ................................................................................................................................. 1
   1.2 Purpose of the Thesis ............................................................................................................................... 2
   1.3 General Information about security in SME ......................................................................................... 2
   1.4 General Information about Security Strategy ....................................................................................... 3
   1.5 Grasping the inner nature of InterAdria ................................................................................................. 5

2 METHOD ....................................................................................................................................................... 7
   2.1 Case Study ............................................................................................................................................... 7
   2.2 Research Method ................................................................................................................................. 8
   2.3 Data Gathering ................................................................................................................................... 8
   2.4 Limitations ................................................................................................................................................. 10

3 CASE STUDY .............................................................................................................................................. 11
   3.1 The Present Security at InterAdria ....................................................................................................... 11
   3.2 Developing a Security Strategy for Special Purposes ......................................................................... 12
   3.3 Why security is crucial for every enterprise? .................................................................................... 12
   3.4 The Gap between Information Technology and Information System ............................................. 13
   3.5 The Gap between IS and IT at InterAdria ........................................................................................... 13
   3.6 Security Strategy for SME’s ............................................................................................................... 14
   3.7 OCTAVE-SM Approach ....................................................................................................................... 14
      3.7.1 Phase 1: Build asset-based threat profile .................................................................................. 15
      3.7.2 Phase 2: Identify Infrastructure vulnerabilities ....................................................................... 16
      3.7.3 Phase 3: Develop Security Strategy and Plans ...................................................................... 19

4 INTERVIEW DATA AND ANALYSIS ............................................................................................................. 24
   4.1 Organizational Level ............................................................................................................................ 24
   4.2 Workflow Level ................................................................................................................................... 25
   4.3 Infrastructure Level ............................................................................................................................. 25
   4.4 Information Level .................................................................................................................................. 25

5 DISCUSSION ............................................................................................................................................... 27
   5.1 Improvements of the Current Situation of InterAdria ....................................................................... 27
      5.1.1 Well-handled situations at InterAdria .................................................................................... 27
      5.1.2 Immediate Changes at InterAdria’s Current Policy ................................................................. 28

6. CONCLUSION AND RECOMMENDATIONS ................................................................................................. 29
   6.1 Key Actions - Recommendation for SME’s ..................................................................................... 29
      6.1.1 High Priorities Recommendation for InterAdria ................................................................. 29
      6.1.2 Low Priorities ............................................................................................................................ 31
   6.2 Reflection ............................................................................................................................................... 32
   6.3 Future Work .......................................................................................................................................... 32

7 REFERENCES ............................................................................................................................................... 33
   Appendix A ............................................................................................................................................... 34
   Appendix B ............................................................................................................................................... 38
   Appendix C ............................................................................................................................................... 41
   Appendix D ............................................................................................................................................... 43
   Appendix E ............................................................................................................................................... 46
List of Figures

Figure 1: Enterprise property classification (own creation) 4
Figure 2: Relevant situations for different research strategies (Yin, 2003) 7
Figure 3: Security wheel (Peltier et al., 2005) 15
Figure 4: Octave in small medium sized enterprises (Alberts & Dorofee, 2002) 16
Figure 5: Hardware platform to fulfill security and protection requirements (own creation) 31

List of Tables

Table 1: Structure of the data gathering (own creation) 9
Table 2: Process 1 - Identify organizational information 17
Table 3: Process 2 - Create threat profiles 18
Table 4: Process 4 - Identifying and analyzing risks 20
Table 5: Process 5 - Develop Protection Strategy and Mitigation Plans 21
1 Introduction

Nowadays the Information is the most crucial component in every business. Security of the information is of the same importance. Every business should be able to compose and to properly implement a good strategy for the security in their enterprise. Strategy for securing the assets should be considered for all major business assets such as: data, personnel and fixed assets. The importance of security is very essential, since it is the key to success and the best way to maintain and prevent attacks from outer and inner threats. Security strategy which is imposed to any kind of business property protects unauthorized access to use, modify or remove a property, no matter if it is a physical asset, or important data. Therefore, security is a very delicate process with which you can deny admission to your business possessions that hold intimated information or that are very important to the enterprise, especially when they are extremely valuable.

Today, many regulations and rules exist are in conformity with the strategy of security such as those in the standard of ISO/IEC 17799:2005. A special treatment is usually delivered to data or information that represents the most valuable position in a business. This happens, because the easiest way to affect an enterprise is by controlling or misusing its property from outside, meaning that there is a possibility to attack through the network. The rule mentioned above is related to specific assets of an enterprise, “data OR information” that present a danger, which needs to be maintained quite well.

The process of securing is a phenomenon that happens all the time and everywhere, although sometimes this process fails. This issue is wide-spread across the world, where people face many problems and difficulties to solving it.

The property of an enterprise of any kind of assets can be divided in two categories:

- Non-secured assets which are inadequate and affects the holder,
- Well-integrated security strategy for assets that are the most valuable and the most wanted systems for every enterprise.

Proper process of security means adequate and safe controls with exogenous and endogenous participants and contacts.

1.1 Problem Definition

The principle of security strategy is to perform well-documented actions that fulfill a predefined plan of an enterprise.

In compliance with security of today’s targeted business industries, the information is the most delicate issue, for which many try to create and develop strategies that could help to avoid any inside or outside factor that could possibly be harmful. (Benson, 2003)

The main problem which is explored in this thesis is that InterAdria doesn’t perform a well-documented security strategy as referred to the paragraphs above. Due to this inconsistency, the enterprise struggles with threats, non regulative processes of security and non coordinative functions within the organizational structure of the enterprise.

Thereafter immediate changes should occur within the enterprise, in the aspect of a security strategy as an integral system, part of the enterprise, which will save the valuable time and costs of the enterprise.
The current structure of InterAdria is not well organized and does not have a proper strategy for securing its valuable assets. The approach which is used to elaborate a new security strategy uses the Octave-sm approach, with which the enterprise can be able to protect information and improve their state of security.

Considering that nowadays every enterprise among which InterAdria is a typical example, must have a security strategy implemented in their business, this problem seems to be very delicate and very important indeed.

The security strategy that is presented throughout this thesis highlights a strategy which is specifically formulated for a midsize enterprise named “InterAdria”, which runs in the market of Southeast European region.

The strategy in name is documented in details, in order to create a process that can be easily integrated in the above mentioned enterprise. The idea of this thesis is to introduce a new security strategy with particular description of data security issue that is adaptable for the needs of the enterprise, which is going to be elaborated throughout this thesis.

This will introduce new innovation techniques that are specifically designed for purposes of InterAdria.

1.2 Purpose of the Thesis

The purpose of this thesis is based on two main points:

1) The investigation of security strategy in InterAdria
2) And the second point is to come up with some recommendations so called ”key actions” which will be suitable and will fit the purpose of security strategy not just for InterAdria but for all SME’s that struggle with the same issue.

1.3 General Information about security in SME

SMEs (small and medium enterprises) are a special type of business that do not just run as small or medium enterprise, but indeed they run more than 90% of the business market worldwide, with employment rate of over 50%. (Allan et al. 2003)

The security strategy implemented in SMEs, for most of them has a very unstable approach considering that many of them try to solve problematic issues of security by not thinking very deeply for future consequences. Instead, SMEs often use online resources that are free, easy to use and that apply a standard security strategy. Since they are willing to implement security data and information systems for their enterprises, it is a chance of providing more facts to convince all participants in necessity of implementation a system which is reliable and secure. This will create secure environment, better and more fair competition and provide success to those which are more inventive, more hard working and more honest. Finally this future SME’s structure will have better and positive impact in society. Below are described some situations related to important data of an enterprise, which are meant to be protected by SME’s security data and information system, although sometimes many factors are not taken into consideration.

Security strategy which will be discussed and studied throughout this thesis, has the aim to deliver a platform, which is specifically proposed for data security.
Below are discussed some issues, facts and strategies of security in SMEs that are directly related to the data.

Many enterprises are thinking of having the remote connection for employees who often use enterprise data, in order to process and store information in a safe remote server. This issue has high importance. If we consider that the information and data bases stored in a PC or laptop has a great risk to be lost, we can conclude that protecting data and information has priority for every single SME entity. In contrary, the remote connection requires Local Area Network for all information stored at servers of the enterprise, or it can require Wide Area Network or Wireless Connection for information stored at remote servers, it would still cause problems of security, knowing that intruders always have the possibility to explore and break the firewalls or any security wall of the network. The strategy of secured data for SME’s, is usually left aside by not having this as the primary issue with high importance. In point of fact the importance of backup, archiving or securing a double flow of information in two different locations is rarely taking in consideration. As a consequence of this, data can be badly affected, thinking of resolving a situation after attacks.

Every asset of an enterprise is of a big importance and has the equal value as data. Related to this issue, a newspaper article written by Solheilm, has pointed out a phrase of Michael Grieves, director of research for the MIS department at the University of Arizona who stated:

“If you don’t discuss security, and you only respond when something happens, that is way too late”.

1.4 General information about Security Strategy

Security strategies are used for many purposes, from which some of the most vital key strategies are related to information in order to: ‘keep it safe’, ‘isolate it from outside intruders’, ‘track every action/transaction’, and ‘videotape every movement inside and outside buildings or offices’.

Security strategies are also to be implemented in every well organized enterprise, which enables them to gain reliability and confidence. Imagine an enterprise which is doing administration services for institutions and doesn’t have proper security strategy! This is one of the reasons why each enterprise needs a security strategy to be incorporated in its infrastructure. This is also very important step for leading the enterprise through a successful road. The next Chapter addresses more security strategies in a specific SME’s. Indeed, a security strategy is composed from many factors which are used or implemented depending on the needs of the enterprise. The figure below shows how the property of an enterprise is classified and where the access control is applied.
To better understand this process, the description below gives an insight view for the property of an enterprise.

**Asset classification** - Classification of assets is a very important step in security chain. Primarily, this component takes all resources and divides them into groups. By dividing and classifying them, the enterprise is able to apply different levels of security in each group, making the security administration run easier within an enterprise.

**Access control** - this component is an important part of security strategies. It is implemented in different areas like:
- Applications
- Routers
- Firewalls
- File Servers
- Room Entrances

The strategy of access control in the enterprise is better to be spread all over the place of assets, because it can be more effortlessly managed.

**Information Security** – the most crucial and the most affected asset is always the data and information. Maybe, it is because there are far much ways to disrupt it, compared to other existing assets of an enterprise. Hence, the security strategy of information is the first matter that preoccupies every enterprise. Peltier and his colleagues that wrote the book for the information security fundamentals, did not really define it with one sentence, instead they used dictionaries which describe what information is in different contexts.

This was a concerning issue to them, so they stated that defining what information is can be comparable to defining infinity.

In their book they try to explain what information security is, and after trying to bring some definitions, they state:
“Currently, information security can cover everything from developing the written policies that an enterprise will follow to secure its information, to the implementation of a user’s access to a new file on the enterprise’s server”. (Petlier, et al. 2005).

**Physical security**- Most of the people are usually concerned with the internet threats that can enter and break into the system. But this doesn’t mean that building a good structure of security in your system can prevent those threats from happening.

Not bragging about the physical security can become a high risk as same as the internet security. A well implemented physical security, can secure all assets from any threat, especially to natural disasters that can be devastating. In contrary, other threats such as thieves sometimes have very easy ways to breaking into the enterprise and harming the system. So this is an issue that an enterprise should be concerned of, because you never know who your enemy is, it can be your employee, it can be a stranger, and overall it can be anyone.

**Personnel security**- Even though this applies to larger companies rather to SME’s, a slight description is given in order to mention this important feature of security strategy which composes the general structure of it.

In the personnel security the one who has to be concerned is the personnel security and not the information security manager. Some of the personnel’s security tasks are: User training, creating job descriptions, performing background checks and recruiting people.

However, if a job describes the position of the employee with security responsibility, than the job of this employee is to take care of everything related to personnel security, including security of people at their job positions.

### 1.5 Grasping the inner nature of InterAdria

The enterprise that I am evaluating for its security strategy is “InterAdria”, an enterprise for software development, telecommunication and education, which today is in need for a more proper security strategy.

InterAdria has been established on 1989, as an enterprise which started to take a market share on software development segment, telecommunication and in projecting field. They immediately started to develop and adapt to the market needs, the Fixed Assets Management Information System. It went through very tough time, during which, they frame worked their activity and perspective.

Today, a significant number of projects for Government Solutions and Telecomm Industry are covered by this SME, such as: Telecommunication Backbones, Telecomm installations, implementation and configuration, system integration, Telecomm Software and Trainings, and as a huge work in Telecomm Industry, their participation with its integration and software implementation is more than 60% of the total works.

Overall, InterAdria is an enterprise in which you can rely on, when you need urgent roll-out in GSM or when you need fast customization of the Software Products.

During the period of last 7 years, they have worked on the structure and organization of the internal form, and it became partner of Motorola, Panasonic, ADC Krone, and also nowadays they are pronounced as an SAP Partner. All this work which kept their relationship with the western developed Europe is to proof their commitment to the perfect work they have done, through all these years.
InterAdria is one of the most often mentioned names in Government Solution’s. With Motorola and Netra enterprise it has realized KPS Network through which around 9000 people are communicating through VoIP platform.

InterAdria has done integration and implementation of the network of 50 PBXs which is the biggest Panasonic PBX network in the World. It has also developed one of the largest payroll software systems that are comparable to the similar software’s in the region, which nowadays runs in the government, exactly in the Ministry of Public Services where it calculates more than 70 000 salaries at once per month.

Its intention is to become a member of the worldwide market, to offer services worldwide, penetrating with the same strength as large and serious companies do.

While this enterprise seems to have a crucial role in software and network area in Kosovo, it also has to have a perfect strategy on how to protect its security of the data, which in the near future will bring the possibility to easily get integrated in worldwide markets.
2 Method

“A method refers to the choices we make about cases we want to study, methods of data gathering, forms of data analyzing, etc. in planning and executing a research study” (D. Silverman, 2001)

Since there are many methods on how to go through qualitative research the chosen method for this thesis is a combination of some of the methods which are: observe, interview and analyze. The aim for observing is to take information and apply them more accurately. There are two types on how to gather information from an enterprise. The first one is doing research and the other one is evaluation. These two approaches both differ from one another. My choice for gathering information and observing more precisely and deeply the situation is by evaluating and preparing the reflections. The purpose of evaluation is collecting information from the enterprise, personnel, etc. and then improving the necessary areas in the enterprise. This also has a crucial role in decision making.

2.1 Case study

The method used in this thesis is the case study method. The definition of case study is presented below written by Yin in 2003:

“A case study is an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident” (Yin, 2003)

Why is this method suitable for this thesis?

Relating to the Yin’s book and his definition of the case study, this method is the most suitable because you have the ability to cover the logic of design, data collection techniques and at the end the data analysis. In other words it can be said that the case study is a research strategy on which this thesis relies on.

To support the question asked above, in the figure below there is an explanation why and when this method should be used.

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Form of Research Question</th>
<th>Requires Control of Behavioral Events?</th>
<th>Focuses on Contemporary Events?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Experiment</td>
<td>how, why?</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Survey</td>
<td>who, what, where, how many, how much?</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Archival analysis</td>
<td>who, what, where, how many, how much?</td>
<td>No</td>
<td>Yes/No</td>
</tr>
<tr>
<td>History</td>
<td>how, why?</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Case study</td>
<td>how, why?</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

*Figure 2: Relevant situations for different research strategies (Yin, 2003)*

From four different strategies which are: experiment, survey, archival analysis, the case study has been the most suitable for this thesis because most of the questions that are conducted are a “how” and “why” type. Going to the two last columns this case has to deal
with contemporary events meaning that the interviews conducted don’t have to do with the historical events. Anyhow, the case study can sometimes overlap with the historical events, which means that the case study can rely on two types of conducting questions: direct observations and interviews. Interviews are the choice of data gathering. Explanation of what kind of data gathering was chosen is described in the chapter below.

2.2 Research Method

Providing a research method which would lead to follow some steps assuring that these steps form a process which helps to define more clearly how to proceed and how to act in a SME such as InterAdria.

Taking in consideration the main factor which is articulated in this thesis, “the security strategy of InterAdria”, a suitable method would be very appropriate and important which encompasses some levels and some clear steps that would help solving delicate issues that concern the security of this enterprise.

2.3 Data Gathering

Two types of interviews are prepared: the Interview with CEO and CIO which most likely are considered as qualitative questioners. The other interviews focus more on the employees and in this case the software department employees. The people that are chosen for gathering the empirical data are so called “strategic group”. To gather up the right and capable information used for further studies, I Interviewed a group of 5 people. The interviews with the CEO and CIO of this enterprise were done using Skype; while they were answering I was writing down all the answers, the other three interviews with the employees were done by mail.

The reason why I chose to do both of these interviews is to come up with some key actions which are the main answer and the purpose in this thesis. These interviews will by no doubt help me go through the security strategy and be focused on the weaknesses that InterAdria has.

The description of the technique on how the data was gathered is stated as follows. There are four main levels in focus. Three phases mentioned in the theory are followed up under each level starting from the organizational level till the information level. These three phases are separated in 5 processes each containing a particular process as described in the theory below. The questions that were prepared for the interviews are divided by each step.

The description of this data gathering technique is shown in the table below. Phase 1 has two processes on which each process have 3 steps. The questions prepared on the organizational level reflect and apply to most of the steps of the two phases (as shown in the table) which are phase number 1 and phase number 3. However some steps of the phase number 3 also apply to other levels which in this case, phase number 3 applies to all of the four levels. This was due to the types of questions made which were related with the theory.
<table>
<thead>
<tr>
<th>Levels</th>
<th>Phases</th>
<th>Processes</th>
<th>Steps</th>
<th>Stakeholders</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Phase 1: Build Asset-Based Threat Profiles, Phase 3: Develop Security</td>
<td>Process 1: Identify Organizational Information</td>
<td>Step 1: Establish Impact evaluation criteria</td>
<td>CEO, CIO, Employees</td>
</tr>
<tr>
<td></td>
<td>Organization and Plans</td>
<td>Process 2: Create threat Profiles</td>
<td>Step 2: Identify organizational levels</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Process 4: Identify and Analyze Risks</td>
<td>Step 3: Evaluate org. security practices</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Process 5: Develop protection strategy and mitigation plans</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Workflow</td>
<td>Process 3: Examining the computer Infrastructure</td>
<td>Step 1: Examine Access Paths</td>
<td>CEO, CIO, Employees</td>
</tr>
<tr>
<td></td>
<td>Phase 2: Identify Infrastructure Vulnerabilities, Phase 3: Develop</td>
<td>Process 5: Develop protection strategy and mitigation plans</td>
<td>Step 2: Select Mitigation Approaches</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security Strategy and Plans</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Process 3: Examining the computer Infrastructure</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Process 4: Identify and Analyze Risks</td>
<td>Step 1: Evaluate impacts of threats</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Phase 3: Develop Security Strategy and Plans</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Table 1</td>
<td>Structure of the data gathering(own creation)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2.4 Limitations

The idea of this thesis stands behind the security strategy of information, developed for purposes of a SME.

While carefully choosing the topic for this thesis there were some areas that couldn’t be covered because of the time limit and the type of enterprise which is SME. The main issue stated in this thesis is how to build up a good security strategy for SME’s which as an example for helping this thesis to clarify the main topic is InterAdria. Some of limitations that must be stated for this particular thesis are.

- Security Strategy touches all the security areas in SME’s which are organizational, workflow, technical and information. It wasn’t necessary to go through each area in depth so the choice was to comprise each security area in extent.
- The best choice was to conduct interviews using Skype even though there was no live observation on how the work goes; I personally worked there in the past so I have a good scope on how the work flow goes and what are the problems concerning security.
- My preference for interviewing staff were certain people on who have more knowledge on security area and that is the CEO, CIO and software department employees. Other departments weren’t involved in the issue of security therefore I didn’t find it reasonable yet helpful to make interviews with other employees.
3 Case Study

3.1 The present security at InterAdria

As an enterprise running almost 20 years, InterAdria has gone through some rough experiences regarding the security of IT from its employees, customers, suppliers and even partners.

The most concerning issue about this enterprise is that its security strategy is not applied. There is no formal Information Security Manager who deals with securing products, including all assets that are processed within its boundaries. The strategy of the communication process between employers and employees has a different approach regarding the relationship employer-employee, which is quite formal in most of the enterprises running in the same region. To be more concise, this relationship can be described as more with friendliness attitude for which the level in the organizational hierarchy is not straight-forward (formal) but it is a two level hierarchy where employees and business managers are present as two separate hierarchical organizational levels, although their conversational status is very non formal.

An example of this organizational hierarchy is the communication process between a client and an employee. In this case a client can have the same communication with the Software Manager and with the Software Developer, meaning that this enterprise does not clearly and formally define the strict position for its employees, which in some cases might result with non-proper functionalities.

Considering this approach of InterAdria towards its employees, they have gained some quite good results when it came to winning new projects, because the prospect always wants to know that there are quite a few people who can be responsible for an issue, so they have the full trust for a developed software or any other service that the enterprise offers. In contrary, the prospect or the client, is always in contact with one person usually, who in many cases does not reply fast, takes slow actions and is not appropriate for that project, whilst with many people in charge for a project, they realized that the client/prospect feels much secured knowing that they can contact you at anytime without hesitation.

This strategy has given InterAdria a very close and friendly attitude towards the internal organizational structure as well as towards the communication with its clients and prospects.

This friendly connection has gone through limits, since there are people who (work on business for security issues) (take care of security) but they do not have time to be focused on security issues of their own Enterprise are always working in different areas, and they can’t be focused just into security issues, knowing that the friendly connection between employees is at some level secured. This form of relation has been applied in this enterprise for many years, since the employee always feels safer and calmer, knowing that many times they are free to ask and even act in an individual way. This method has shown much success for the enterprise although for some cases it resulted with failure.

What InterAdria has experienced was an internal threat. One of its programmer employees was working on open source software which was in the hand of all the programmers in that time. Here is the biggest mistake that they have done, trusting every employee.

First of all, it didn’t divide the software into parts and for each part there should have been some rules that the employee (the programmer in this case) wouldn’t have permission to have access in the other parts of the software. It should have been password protected for
every part, which in this case, the software was password protected for all of its usage. While this is a big concern for InterAdria’s future, a decent proposal to a solution is presented in this thesis. This proposition would lead this SME at another stage of its organization, where security would be the main developed and well maintained aspect, by be implementing the proposed strategy in a proper way. InterAdria has developed in-house its software product portfolio and has a great concern how to keep data secure and how to back up everyday work. One of the mentioned issues is solved. The other issue is to solve protection of source codes of the in-house developed software products. The third challenge is to build up a secure and controlled access to the server site and finally security of each working station in InterAdria network.

3.2 Developing a Security Strategy for Special Purposes

The intention of developing a strategy, is to help InterAdria and all it’s members of the professional security body, to develop and in some aspects to redevelop the strategy of availability, integrity and confidentiality of information, including business information, software sources and databases. The strategy consists systematic approaches that would lead all administrators, engineers and developers to launch security policies within InterAdria in a proper manner.

The current situation of InterAdria’s security strategy is the following:

- Security of the fixed assets and inventory is not at risk. Proper burglary alarm and very advanced CCTV system with capacity of 250 GB data storage is installed.
- Data and information security is at risk. There is no proper security for the access to the data in the server. Also proper firewall system is missing.
- Physical access to the server and working stations is possible. Therefore, there is a risk of physical damage.

3.3 Why security is crucial for every enterprise?

Each enterprise within its assets and equity has also very important source of data and information which normally should not be exposed to public. Especially, data which has been build-up and developed through very complex and long process of development needs to be protected and secured. Today, not only intentional risk of damaging and stealing data and information are present. Among others, very big threats are also risks from Viruses which can damage entire DB and Information system. It is not to be underestimated the risk from all kind of disasters. Different from these disorders as stated above, cyberspace attack is another issue that can be very harmful indeed. Enterprises can be in the highest risk by pretending that this attack is very rare to happen. Every enterprise must always make sure and re-enforce their security in every perspective. So, being vigilant is the right decision to avoid failing but not being vulnerable with the software, because the easiest way to have an attack from the out known hackers is when vulnerability is present in the enterprise towards the system. The security itself should always be taken in consideration by all people who take part in a business, in an enterprise. In point of fact people of IT and people of other departments should adapt to all security values and should take care of it.
This is with high importance considering that many times security itself is neglected by people and there is not a proper communication which easily leads to unwanted interferences. In a scenario of one of the mentioned actions, protecting data and information is a big challenge. Avoiding the bad experience, this risk should be minimized. The only way of minimizing this risk is implementation of Security strategy. The Security strategy, therefore is very crucial and the security should be enough capable to reach its highest capacities whenever it is needed.

In the subsections below the gap between departments (Information Technology and Information Systems) is articulated, in order to present this concern, how it happens, why should people of different departments be aware of the rules and the communication between one another?

3.4 The gap between Information Technology and Information System

One of the most concerning issues today, in many large enterprises is the gap existing in between IT people and IS people. Many companies are preoccupied with this concern, trying to find the right method and the right solution to escape from such situations. This dilemma is related to business processes that effect the whole business when IT and IS are not well coordinated. These troubles within an enterprise happen as a consequence of misleading the organized processes that are pre-located in the enterprise. The gap of IT and IS usually effects enterprise function’s, considering the side effects that never has a clear view with how information is being processed, and how the communication is being conducted between IT and IS. These effects can bring an enterprise to very unpleasant situations, especially these companies that compete at intense industries or those that are very much dependent on the IT sector of the enterprise.

3.5 The gap between IS and IT at InterAdria

From the observation done at InterAdria, the gap discussed in the section above is exactly the issue. InterAdria has disequilibrium between its people concentrated in Information Technology, who in most cases are much closed and not talkative, and people of Information System who try to organize processes not just in the IT sector, but are also present for business processes. In this case, the hard work is more performed by IS people that try to get integrated with every sector and in every aspect of the enterprise. In contrary, IT does not help very much in this matter. IT people try to finish their job, try to do their best, but usually they do not inform details for the finished work to IS administrator. In a well organized IT sector of InterAdria, IT people should be more competent on the processes and actions they take. They should also be competent on their reporting, which should be done on daily or weekly basis, informing the IS sector for the most updated/current situation in IT. This matter is of a big importance for the whole strategy of InterAdria, because it easies the business processes and the relationship of communication in between IS and IT. Since InterAdria belongs to Small medium sized companies an appropriate solution toward a security strategy is described in this chapter. Even though the most famous established
standards are: COBIT, Marion, ISO/IEC 1779:2000, ISO/IEC 13335, British standards, etc, these standards however are more suitable for bigger companies which didn’t match the needs of InterAdria.

For a better approach regarding security strategy a very suitable method for all kinds of SME’s is used. The method is called Octave-sm (The Operationally Critical Threat, Asset, and Vulnerability Evaluation), the “SM” stands for small medium size companies, which is conducted particulary for Small Enterprises that has less then 100 employees. It is a very useful approach since it’s a self directed approach and it can include 3-5 people in the enterprise to establish their security strategy. The people that are involved in planning and conducting a security strategy plan must be personnel that have broad knowledge on how the enterprise works, and it is more likely to have personnel in two different areas: in the business area and in the IT department.

The idea for choosing this method is that this method has a combination of IT security IS security and Information security all of these are a categorized as sub levels of security strategy which.

3.6 Security Strategy for SME’s

To conduct a security strategy for small medium size enterprises needs a lot of time and a very deep investigation and observation. In these days the approaches towards the security strategy in one enterprise has been evaluated mostly for the large enterprises and the idea for implementing a security strategy for SME’s is needed as well since many enterprises lack on knowing how to address technological aspects on security risks evaluation. Usually the small enterprises have a flat nonhierarchical organizational structure and the staff members must be highly skilled in every area. Another flaw for small medium enterprises is the lack of the staff which results on the limited time for improving the security conditions in the enterprise. SME’s usually have a tight budget regarding the security area in the enterprise so a proper solution for improving this weakness would be the approach that it is used and that is the Octave-sm approach. This approach is an efficient and inexpensive approach which is designed and constructed in an easy way to be followed, since it can be implemented just by highly skilled team members of the enterprise. Hence, the SME’s mostly perform outsourcing activities; a decent approach such as Octave-sm, can lead these types of enterprises to address their technological aspects in the side of activities dealing with tangible and intangible assets.

The everyday work which deals with different communication activities reflects the overall situation of the enterprise. The importance of communication is dependable on the system of the organized structure for securing all activities with no undesirable effects.

The main qualities for security are: confidentiality, integrity and availability. Sustaining these qualities a conclusion for an appropriate solution which is divided in four layers/phases is stated below:

- **Organizational level** -Mostly this level deals with Strategies on IT security, Decision making, Risk Management. SME’s seldom implement an IT security strategy. For this reason the best way is to encourage the SME’s all over the world to try and adopt a strategy that fits their organizational level. This will help the management of the enterprise assess the role and importance of IT security.
• **Work Flow level** has two major aspects: the security and dependability workflow. The workflow level is more a process oriented level. The former mentioned aspect of workflow is more concerned with the security of workflows like the customer care while the latter is more about workflows that manage the security.

• **Information level** deals with access control, user rights, federal identity. The most important facts in information security are the information policies and I really support the author’s definition on the importance of information policies, he quoted:

”If information security were a person, the security policy would be the central nervous system.” (Peltier et al., 2005)

Policies are the main thing in information security and provide a good structure to the system. To have a more clear view of Information Security here is the picture that tells how the security policy has such a big impact in one enterprise.

![Security Wheel](Peltier et al., 2005)

• **Infrastructure layer** deals with the network security, hardware, viruses, worms, etc.

I purposely took these four layers because it will help conducting the interviews with the staff of InterAdria. The interviews will also have a good structure combining Octave-sm approach and these four layers.

3.7 OCTAVE-SM Approach

"OCTAVE is a risk-based strategic assessment and planning technique for security.” (Alberts, Dorofee, Stevans, Woody, 2005)

For going any further on the Octave-sm approach, the members of the enterprise that are obliged to take actions on applying this approach must work together and decide if everybody agrees that this is the approach that is suitable for SM enterprises. If so, than they must continue focusing on the security needs of the enterprise and focus in three key aspects: ”operational risk, security practices and technology” (Alberts et al., 2005)
Why is the Octave-sm method the right solution for SME?
First of all the Octave-sm differs from the OCTAVE method which is used for larger companies and the implementation is done in a deep and thorough way. The difference relies on the fact that in the implementation of Octave-sm we can use three to five people which have access and knowledge in each department and are familiar with the enterprises business processes. This is exactly InterAdria-s cases which there are not many rules on whose members should be focused in one department, but else certain members have broad insight on every department. Selecting the appropriate members of an enterprise to conduct a security strategy in SM enterprises is very crucial since their relations must be open and confidential to other employees. The team members can be managers and staff members that work closely together and know what are the main weaknesses in the enterprise. It is better to include both from business and technology side. There are some principles that must be followed in order to have a better collaboration within these members.

- Communication skills
- Knowledge of the business and information technology environment
- How does staff use the information technology in the enterprise
- Good relations between members
- Leadership (manage the group for meetings or give instructions )

By using OCTAVE-sm the enterprise will have protected information and improvement of their state of security. There are three phases that the author of the book”Managing information security risks”Alberts has stated:

- Phase1: Build asset based threat profile
- Phase2: Identify Infrastructure vulnerabilities
- Phase3: Develop Security Strategy and Plans

Each phase has some Processes that must be followed.

![Diagram](Figure 4: Octave in small medium sized enterprises ( Alberts & Dorofee, 2002))

### 3.7.1 Phase 1: Build asset-based threat profile

The first Phase focuses on the evaluation of the risks and pinpoints the assets and evaluates the current security in the enterprise. This phase has two processes and each of these processes have some activities in which we must follow in order to come up with the right solution towards the security strategy:

**Process 1: Identify organizational Information**, this process is more concerned about the organizational assets that should be identified for any risk impacts, this process also has some steps that we should go through.
<table>
<thead>
<tr>
<th>Steps</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step1: Establish Impact Evaluation Criteria | This concerns
• Impact
• Impact value
• Impact evaluation criteria |
| Step2: Identify Organizational assets      | The most important factors in the organization are:
• Information
• Services and applications
• Systems
• People |
| Step3: Evaluate organizational security    | A security practice survey enables an analysis team to evaluate the extent to which security practices are reflected in the way its organization manages security. |

**Table 2:** Process 1- identify organizational information

**Step1:** An **Impact evaluation criterion** defines the different risk impacts in an organization. By establishing this step we protect the organization from many risks that can occur. In this step we define some measurements of the impacts below:

• Reputation/customer confidence
• Safety/health of customer
• Fines/legal penalties
• Financial
• Productivity

For each impact we must define three types of measurements which are: low, medium and high. In the impact of the reputation and customer confidence we must measure how the reputation and the customer loss are affected. There are three impacts that should be evaluated. In the reputation case the impacts for low, medium and high are:

• is the reputation affected minimally,
• is it damaged but can be recovered and
• If the reputation is destroyed and cannot be recovered.

We must define in which of these three impacts the enterprise fits concerning the reputation. These impacts must be fulfilled when a company wants to conduct a security strategy. For life and the health of the customer we must take in consideration and measure these impacts: the life of the customer or staff members (this includes threats of their lives), health of staff members and Safety. For Fines and Legal penalties we have these types of impacts that must be measured: Fines, Lawsuits and investigations. For the Financial part we must define the operating costs, revenue loss and one-time financial loss. And for the last one which is productivity we must fulfill the right impact which shows the staff hours more concrete on how many hours per day they work.

**Step2:** For identifying the organizational **logical and physical assets** include information, services and applications, systems and people.
There are some questions that need to be conducted in order to have a comprehensive view of the enterprise assets. This part will be applied in the interviews concerning SM enterprises.

**Step 3: Evaluation Organizational security practices.** This part is quite important since it enables the evaluation of how the enterprise manages security by defining which security practices are reflected and used.

Some areas that are included in the evaluation of how the enterprise manages security are described below:

- Security practices help the enterprises initiate a security strategy.
- Organizational vulnerabilities show the weaknesses in the organizations policy.
- Catalog of practices includes both strategic and operational security practices.
- Strategic practices are focused on organizational issues more concerning the policy level and business related issues.
- Operational practices different then strategic practices it is more concerned of technology-related issues.
- Spotlight status shows us how the enterprise is performing in the security level.

**Process 2: Create threat profiles**

<table>
<thead>
<tr>
<th>Steps</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: Select Critical Assets</td>
<td>By selecting the critical assets in the enterprise we must discuss the operation aspect of each asset:</td>
</tr>
<tr>
<td></td>
<td>• Who controls it?</td>
</tr>
<tr>
<td></td>
<td>• Who is responsible for it?</td>
</tr>
<tr>
<td></td>
<td>• Who uses it?</td>
</tr>
<tr>
<td></td>
<td>• How is it used?</td>
</tr>
</tbody>
</table>

| Step 2: Identify Security requirements for critical assets | This include the security requirements which are: |
| | • Confidentiality |
| | • Integrity |
| | • Availability |

| Step 3: Identify threats to critical assets | perform a gap analysis of the areas of concern you elicited earlier in the evaluation |

**Table 3: Process 2- Create threat profiles**

**Step1:** This phase enables us to select the most important assets in the enterprise. The analysis team should consider four main questions that concern the importance of assets. We must detect which asset will have an adverse impact in the enterprise if the following occur:

- The asset is revealed to an unauthorized user
- The assets are modified without permission
The assets were lost
The access to the assets was unable

By going through these four questions the analysis team must define which assets have the biggest impact in the enterprise when these threats occur.

**Step 2:** Security requirements that are important and that are typical for any enterprise are:
- Confidentiality
- Integrity and
- Availability

**Confidentiality** is the limitation of accessing the system without the permission, unauthorized users have a limited access to the certain data which include personnel information, proprietary business information. There are some procedures that should be implemented for maintaining the confidentiality. The most important goal in confidentiality are authentication methods which include User Id and passwords, authentication and authorization. Some known threats to information confidentiality are: viruses, malware, unauthorized user activity, etc.

**Integrity** of the data means that the system must be protected from unauthorized modification of data. Data integrity means that the data has been changed whether by accident or it was a malicious activity. For the reaching the integrity control there are three principles which are used:
- Granting access on a need-to-know basis
- Separation of duties
- Rotation of duties

**Availability** means that when certain authorized users need something in their system it must be assured that it is accessible for that matter. Sometimes it happens that the user can’t get to the data he/she needs and that can be affected by some technical issues or human accidents in the system. There are two aspects of availability:
- Denial of Service
- Loss of data processing capabilities as a result of nature disasters or human actions

**3.7.2 Phase 2: Identify Infrastructure vulnerabilities**

The second phase is for reviewing the infrastructure of the Computing. The team members that are responsible for the analysis should do evaluations on how the computing infrastructure is used by employees in order to have access to important assets.

**Process 3:** This process examines the access paths in the infrastructure for critical assets and analyzes the process that are technological related with the infrastructure. It is vital to know which are the critical assets in the enterprise. In this step we must define one of the most critique assets starting from network access paths. This path enables the access of systems, devices, information in one enterprise. In order to build and to go through this process the enterprise should have highly skilled employees which has the appropriate skills on computer networking. However, this process is not obligatory for the security strategy and because of that, this will lead to a short description of this process and focus more on the other two upcoming processes which
are critique for every SME’. The importance of this process is: examination of access paths and the analyze of the technology related processes.

3.7.3 Phase3: Develop Security Strategy and Plans

The third phase is for analyzing the risks of important assets and to decide what action to induct. When the exact information is gathered the team members conduct a strategy for protecting the current assets. This is the last phase. After you gather all the information needed for the evaluation in this phase, you start to develop security strategy and risk analysis.

This phase is consisted of two processes which are:
- Process 4: Identify and analyze risks
- Process 5: Develop protection strategy and Mitigation Plans

**Process 4: Identifying and analyzing risks has 3 steps which are critical to go through.**

<table>
<thead>
<tr>
<th>Steps</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step1: Identify the impact of threats to critical assets</td>
<td>The analysis team are concerned with the threat outcomes (disclosure, modification, loss, destruction, interruption). The impact description is a narrative statement that describes how a threat ultimately affects the enterprise's mission.</td>
</tr>
<tr>
<td>Step2: Create risk evaluation criteria</td>
<td>This time there are three types of evaluation criteria: high, medium and low. We must pin point all of these impacts in some of these evaluation criteria.</td>
</tr>
<tr>
<td>Step3: Evaluate the impact of threats to critical assets</td>
<td>The combination of a threat and the resulting impact to the enterprise defines the risk to the enterprise. The analysis team reviews each risk and assigns it an impact value (high, medium, or low).</td>
</tr>
</tbody>
</table>

**Table 4: Process 4 – Identifying and analyzing risks**

**Step1: Identify the impact of threats to critical assets**

To provide some links between the threat and assets in the enterprise we must make a kind of descriptions os some impacts that can go from threats to the critical assets. This process is related with the other process and especially with the process number 2 which is Create threat profiles. In order to go further on with this step we must look at security requirements and threat profiles for each critical asset.

There is an outcome which means that is a result of a threat that can influence in the critical asset. There are four types of these outcomes: disclosure, modification, loss/destruction, and interruption. For a better understanding of the affect of these outcomes the authors of the book Managing information security risks explained:

“Someone inside the organization uses network access to deliberately modify the medical records database. This could result in patient death, improper treatment delivered to patients, lawsuits, and additional staff times to correct the records.” (Alberts, Dorofee, 2002)
This leads to the step 1 of process 1 which the impacts that are mentioned there should be taken in consideration during this step. Those impacts are:

- Reputation/customer confidence
- Safety/health issues
- Fines/legal penalties
- Financial
- Productivity

All of these impacts should be adapted in order to meet the enterprises needs.

**Step2: Create risk evaluation criteria**

To define an evaluation criteria the focus must be on the same impacts as the above. This time there are three types of evaluation criteria: high, medium and low. We must pin point all of these impacts in some of these evaluation criteria. For example if the reputation irrevocably is destroyed and damaged then this is categorized as a high level and the people who conduct the security strategy must take immediate action to recover this problem. This lead to placing all the risks in the enterprise in these types of levels: high, medium and low. To do this the easiest thing is to work on the Octave-sm worksheet which the authors have planned a perfect security strategy on which you can work by your own.

**Process 5: Develop Protection Strategy and Mitigation Plans**

<table>
<thead>
<tr>
<th>Steps</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step1: Describe Current Protection Strategy</td>
<td>This step will show us how the organization can act, implement and maintain the internal security</td>
</tr>
<tr>
<td>Step2: Develop Risk Mitigation Plans</td>
<td>Mitigation plans are very important since they tend to reduce risks to critical assets by first noticing the threats</td>
</tr>
<tr>
<td>Step3: Create action list</td>
<td>An action list defines any action items that your team members can apply to the organization without the need of training.</td>
</tr>
</tbody>
</table>

| **Table 5:** Process5- Develop Protection Strategy and Mitigation Plans |

**Step1: Describe Current Protection Strategy**

Information security is critical for every enterprise, this step will show us how the enterprise can act, implement and maintain the internal security. To implement a protection strategy in SME’s, it is likely that the enterprise have limited funds. The following practice areas are included in protection strategy, however these areas are not very reliable in SME’s since we are focusing in security strategy which is a subset of a strategic practice area. In one word the protection strategy is an organizational level which more likely is structured to strategic practices areas which are:

1. Security Awareness and Training
2. Security Strategy
3. Security Management
4. Security Policies and Regulations
5. Collaborative Security Management
6. Contingency Planning/Disaster Recovery

Each of these areas are subdivided into some characteristics. Since the focus is in security strategy here are some questions that must be answered in order to fulfill the criteria’s of this area:

Are there any security issues that are involved in your strategy? What is the way to improve how security issues are integrated in the strategy of your organization?
The same questions are stated also for the business issues. To describe the current protection strategy the 3 first steps must be fulfilled in order to proceed further.

Step2: Develop Risk Mitigation Plans

Mitigation plans are very important since they tend to reduce risks to critical assets by first noticing the threats. When it comes to developing mitigation plans are known for detecting threats when they develop, prevent threats from developing and recover from threats after they develop. A suggestion is to structure the mitigation plan for the most critical assets in the enterprise. To develop a mitigation plan first of all you must select a mitigation approach which in this step you must define what is needed to be mitigated. If you mitigate a risk then the action is designed to reduce the risk but if you accept the risk (if it is not very harmful) and if you don’t take any action to mitigate that risk then you must deal with the consequences. You must evaluate some answers to your enterprise and if the enterprise is accepting the risks then you must state if those risks have low, medium or high impact values? The best way to proceed further is to accept risks with low impact values but to strictly mitigate those risks that have high impact values because the point of this step is to eliminate all the threats towards your enterprise. After you choose the approach on how you mitigate risks, then you should take some actions that recognize the threat as it is developing, resist the threat from developing and prevent from the threat after developing.
To reduce the risks to those critical assets you could implement three types of practices: administrative, physical and technical. After you recognized which assets are priority to be mitigated then you examine the cost and benefits of those actions to know that if the enterprise is able to support that mitigation considering their budget.

Step3: Create action list

To create an action list it is not necessary for a specialized training or change of policies in your enterprise. To organize a better security posture in your enterprise it is better to start implementing action items.

To make an action list you must consider the following actions:

- Near-term actions that need to be taken
- The person responsible for completing each action item
- A completion date for each action item
- Any management support that is required to facilitate completion of each action item (Alberts & Dorofee, 2002)

When you create the protection strategy and risk mitigation plans then you must review your action list and see if they are appropriate actions for implementing those protection strategy and risk mitigation plans.
When you pinpoint the action items for conducting an action list then a responsibility needs to be assigned in order to complete the critical needs of your enterprise. Some of the following questions need to be addressed to see if your enterprise is capable of completing those actions. Who will be the person responsible for action items? Or When does the action need to addressed?
4 Interview data and Analysis

The empirical data has been collected using interviews with the CEO and CIO of the enterprise and mail interviews with the three employees of the software department of InterAdria.

The intention of these interviews based on different hierarchical levels of the personnel of InterAdria is to provide a group of questions which will be prepared in accordance with the Theory phases and the Method used.

In theory which is described throughout this thesis, specifically mentioned in Section 3, there are three phases, each running with one or more processes including the third level running with steps based on each process.

Concerning the four levels in conjunction with theoretical approach will form a group of interviews that will act as structurally performing for the next processes that should be implemented in the strategy of InterAdria. This strategy of placing specific questions leads to address more delicate issues that are currently present at the enterprise.

Interviews which are based on the theoretical approach are organized based on the flow of the theoretical hierarchy of phases, processes and steps, therefore for each step a level is introduced telling to which category it belongs by giving a question that is related only to the phase / process /step and more specifically to the predefined step of the theory.

4.1 Organizational level

The first level identifies the most important assets in InterAdria that need to take immediate action. The majorities of questions are conducted in the organizational level which includes questions from phase number 1 and phase number 3. Mentioning some of the most critique questions for InterAdria will help this thesis achieve the key actions which are stated in the end as a recommendation for a better performance and a better security in the future.

Considering the question number three:

“Related to Security, how do you practice it and is there any proper security performance that is strong enough to protect yours assets, your people and your enterprise in general?”

Both the CEO and the CIO of this enterprise weren’t satisfied with how they practice their security. In which the CEO stated that they have built a trust upon employees regarding the security of any internal threat which this trust lead to some internal threats in the past, although they have security cameras and alarm systems this doesn’t stop the intruders for doing harm both internally and externally. Related to this question the CEO of InterAdria also said that the most vulnerable assets that this enterprise have are the software’s. He stated:” the current security status of our products is in a critical situation which we need to solve fastly especially for the internal threat”. This means that they are in desperate need of protecting their most delicate and valuable assets otherwise more threats will happen in the future. As it seems the enterprise is well prepared if physical assets happen but they mostly are conserend of many internal intruders.
4.2 Workflow level

The most important questions that are addressed to the workflow level for the interviews of CEO and CIO are discussed in this part. The question addressing the workflow level is about “the risk analysis and what actions do they (staff) take for avoiding these risks and do they think of any side-affects such as: reputation, financial, productivity or even fines?” The response from the CEO was quite informative saying that the risk is always present and especially in SME’s like InterAdria which have to take risks and mainly when applying for tenders where you rather win or you don’t. Related to this, he stated that they also have risks in their development process of their product portfolio. Because of the importance of this issue, InterAdria has concerns regarding the proper actions on how to articulate the right plan for asset protection. The plan they own now is a general plan for all assets including their maintenance and protection. This, however doesn’t mean that they will stick by this general plan on the future since their most delicate assets are at risk and they need a better solution for protection.

4.3 Infrastructure level

The important notice that is likely to be stated here is the following: if “InterAdria organizes its infrastructure in a way that there is a predefined way of accessing its assets “the answer came pretty straight forward from the CEO who said that they do not have any structured plans on how they can protect unauthorized access to their assets (data, source codes) and they are waiting for a new plan in the future. One of the questions that are more relevant and important for infrastructure level is stated below ” how the enterprise divides the responsibilities for their most critical assets?” the enterprise seems to have a great partition when coming to the responsibilities that the employees have for the assets. There are 4 people in charge of the security which are responsible for different assets.
Yet, another important question is stated concerning the risk and how the enterprise measures the risk. The risks are categorized from the lowest level to the highest level.

4.4 Information level

Information is one of the critical assets when it comes to implementing a security strategy. The question prepared for this level is more about the future of InterAdria’s work and what are their plans and actions for proceeding through a more strategic security. The last question is however a combination of all these levels.” About your future plans. Do you think there is a need to upgrade your security strategy frequently by maybe investing in the latest technology including hardware and software and do you plan to refresh your personnel by giving extra trainings or even employing new skilled members that should deal with such activities?”
The answer was pretty clear that this enterprise will want to take actions towards a better security which would led to training the employees upon how to act towards different threats and preparing their staff with the latest technology that lead on integrating in any development.
4.5 Security strategy in SME

Going through the security in SME’s and observing their situation helped me for a better solution towards security strategy in my particular case of a SM enterprise which is InterAdria. In my opinion the security strategy in SME’s is a status –quo and this need to change since there are dozens of threats in this world that can cause heavy damage to these enterprises. Gathering the data and observing the situation in this SME I might say that it was a bit tough since I didn’t have any live contact except using the skype for the interviews even though I have worked in this enterprise for 1 year or so and I was determined to write a thesis which would be helpful not just for InterAdria but for all SME’s which are in the same situation concerning security strategy. Choosing the Octave-sm approach as my theory helped me understand more of what are the needs for security in SME’s.
5 Discussion

5.1 Improvements of the current situation of InterAdria

It is clear that the issue of security is in urgent need to be transformed with new reforms that could help to avoid such threats that already happened.

What is to be summarized from the current situation in InterAdria was the concentration in the theory which would probably transform some critic situations that are already present there and are related to each department.

The answers from the interviews conducted have taught me many things that are present at InterAdria. In some aspects they are well-handled, in the other hand they need an immediate improvement in the structure and in the way the business in general is managed and how the owners are maintaining it. Below some facts are given that are related to answers of the Interview 1 and Interview 2. These facts present the well handled situations as mentioned above and those that need an immediate improvement.

This analyze binds together the ideas behind the theory with the answers given by InterAdria employees that primarily help me to bring conclusions related to the situation of InterAdria, and secondary to propose new solutions that would be for the good of this enterprise, to change some structural elements that would help to increase and improve the process of development with faster steps.

5.1.1 Well-handled situations at InterAdria

The Octave-sm approach in general tells us about the communication and the proficiency of the personnel who runs the business. In reality, the observed answers from both interviews tell us that within the enterprise and in opposite with customers the communication is handled very well which in fact the enterprise has a good reputation especially to big customers throughout the country.

As for skilled personnel, the business itself of this enterprise tells how proficient these people are and how good they maintain their knowledge by updating it with new skills everyday. Starting from the owners who have very high knowledge for business rules, economics and laws, tells how successful this enterprise was and is still being through this 20 years work experience.

Employees are also very high qualified, especially those that are project managers and leaders of groups of people, who perform and run big projects in Telecom, Government and other well-known companies.

In OCTAVEs the issue of knowledge is well articulated and it gives a brief description why it is important. In fact, this importance is clear by simply comparing its definition in OCTAVEs with ongoing business of InterAdria.

Different from what is said above, the assets which are mentioned many times in OCTAVEs and in the interview as well, it is clearly understood that employees and the business runners of InterAdria give a high value to their assets specifically to those belonging to the software department as in-house-built assets, and those of telecommunication.

They seem to be very aware of what they own, how valuable these assets are and that they should be very careful with them. Actually, they try somehow to tell that they need changes
to their strategy or they need to add a specific and clear strategy which should be prepared in a good way and which should be present in every aspect of security within the enterprise. They think that the value of their assets somehow should be followed by a perfect strategic plan. The purpose of this plan is that it can help them to avoid interruptions, misunderstanding, abuse or any related issue. This plan is very important to them, for some with very high priorities and for some in urgent need to be formulated; in general it means that they are pretty aware of what they want for their structural organization matter of the enterprise and their assets.

5.1.2 Immediate Changes at InterAdria’s Current Policy

According to OCTAVEs approach, the structural and organized plan followed by detailed description of processes and steps that should be performed, tells one of the best ways to keep an enterprise protected and in a good shape.

In the case of InterAdria, it’s a bit hard to say that they are ready to follow a plan which is specifically structured for them, in order to keep the flow of the work in order. In fact, InterAdria currently is not following any structured strategic plan for their security and for their development stage of their valuable assets.

Therefore based on OCTAVEs approach the five processes are indispensable and should be applied at InterAdria for improvement purposes that can help to eliminate threats and structure non-organized assets.

What is understood and extracted from the answers of both interviews, it is clear that the employees and the enterprise itself do not use regulative predefined rules which should form the daily work for everybody, and instead they use a friendlier attitude in order to keep the enterprise in a good mood.

But, what exactly the OCTAVEs five processes could affect the enterprise? First of all, the enterprise will learn a new way of working, this is important for its employees who should know that there is a strict rule and that they should be aware of. This example can help the enterprise to get easily upgraded with new developed products, because accompanied by a rule, all workers are aware of how to act, what to work, when to finish and when to have fun. In the case of InterAdria, the 24/7 friendly communication sometimes seems to be non-formal and not effective in the work time.

The figure represents some steps that should be created in order to develop and create asset profiles that are based on a strategic plan for their protection. InterAdria basically needs a general strategic plan which consists of structured rules that should be known, performed and accomplished by every employee. Working in this order it is much easier to create new plans related to security as described in OCTAVEs approach and achieve reduce of risk of their assets and their personnel to the maximum.

In the section below, the main key actions with high and low priorities are presented, in order to provide a better overview of what can InterAdria improve immediately or in their near future.
6. Conclusion and Recommendations

The focal point of this thesis is concentrated in one main topic of “security strategy”. In fact, this security strategy is unfolded for the purposes of improvements and new recommendations that would challenge the current situation of the studies enterprise throughout the thesis.

Regarding the development process in the security area of the studied enterprise, below are presented some actions divided with high and low priorities. This division is done based on the actions that need an immediate transform “high priorities” and those that can be affected after the priorities are taken in consideration.

These proposed changes that should be taken through the below mentioned actions are extracted from the collaboration I had between the employees and from some statistical data that are gathered from the answered interviews.

6.1 Key Actions - Recommendation for SME-s

Related to the analysis brought by interview answers of both structures of employees (business runners and software engineers/developers) it is much clearer how the situation should be preceded and what actions should be proposed for InterAdria and other Small and Medium Size Enterprises. These actions should strengthen their structures, confidence and reliability and lift them in higher business levels. Below, several issues with high priority are presented, which urgently need’s to be deployed.

Below are presented the key actions that should be taken in consideration when talking about outside and inside factors that intentionally or unintentionally try to harm the enterprise, intentional attacks, natural disasters, and other accidents that can do damage to 100% divided with high priorities and low priorities.

High priority actions are the main issues which should be analyzed by InterAdria for implementing and using the proposed strategy.

Low priority actions are in second level of importance which should be analyzed and implemented after the high level actions are performed.

6.1.1 High Priorities Recommendation for InterAdria

1. The IT infrastructure requires new protection of information.
   - Security administrators should spend more time to structuring the security policy within the enterprise.
   - The enterprise should decide how much time and effort must be spent weekly concerning the security issue only, creating a calendar that helps to concentrate the power for this delicate issue as well.
   - The IT infrastructure needs more investment for building strong security with new server room, powerful capacities and strong security software.

2. Introduce the new policies and new security software for every internal clients/employees of devices.
   - Build up a new strategy and new working procedure for employees.
• Install security software for every computer user, especially those who deal with important information.
• Create a human controlling system by the administrator of IT, to check more frequently the work of employees.
• Bring up some new ‘strict’ rules such as: the private email should not be used during working hours, any external hard drive coming outside of the offices should never be put in the hardware, and developed products can never be taken outside the offices of IT, unless it is given with special permissions.

3. Install security hardware for natural disasters protection.

4. Install security hardware in the secure place to recover data and information from natural disasters. Implement: “Disaster Recovery System”.

5. Create passwords for every single transfer and connection to the local network.

6. Investigate and create log files for every transaction happening within the local network in connection with wide networks.

7. Create an external server (See Picture bellow), outside offices, where every single transaction and every data is replicated.
   • The Disaster Recovery System (server) should be placed in a secured place with 24/7 online connection with the main server room.
   • Use the network controlling system for threats that might enter in the network line.
   • Always check every Internet Protocol that tries to connect to any of the servers.
   • Use strong firewall system and virus protection software, in every server and every client.
After describing some of the most important key actions that need to be performed in InterAdria, and after analyzing the threats and the current position of IT and IS infrastructure of InterAdria, the low priorities are presented below which can be left for some time, until the key actions/high priorities are implemented.

6.1.2 Low Priorities

1. The enterprise should be able to create special informing events for its employees in order to inform them about the information, its importance and consequences if abused.
2. Time to time trainings specifically for IT and security administrators, who need to know more in depth the issue of importance that information has.
   - Trainings should also be organized for teaching users how to maintain security policies, security strategies, how to test these systems and how to know more tactics in relation to security that needs to be handled.
3. Evaluation of the practice executed in the security area of the enterprise.
• Administrators, developers, testers should provide a good feedback with more knowledge on how to handle and secure information under any attack.

6.2 Reflection

The main purpose of this thesis which was to bring up some new ideas based on regulative approaches such as different existing security techniques, methods and theories has been achieved. The base for formulating a strategy that could conform to the needs of the enterprise is articulated in the theory and the method section where the OCTAVE-SM approach is in the main focus for bringing out new ideas and possible effective results in the future of the studied enterprise.
Regarding the new improvements that should be done, the OCTAVE-SM should reflect positively based on what has been proposed to be changed. Accordingly, these changes include some advanced features that are not present in the current situation of the enterprise. Instead the analysis section where it is clearly stated what is wrong and what isn’t wrong in the enterprise might clearly open new opportunities for the enterprise to change the structure and the enterprise method that they currently have.
Of course that rules or regulations regarding security issue which are also mentioned in the Introduction of the thesis where the standard “ISO/IEC 17799:2005” is stated, can supervise the enterprise for adjustments and rearrangements in their current security conditions.

The purpose of the thesis under the introduction section is stated with two main points:

1. The investigation of security strategy in InterAdria
2. And the second point is to come up with some recommendations so called ”key actions” which will be suitable and fit the purposes of security strategy in InterAdria

Have been fulfilled and explored during the research period. The first question regarding the security strategy of InterAdria is well consolidated all over the work of this thesis. This issue has been studied deeply and now it is a clearer view for the enterprise’s security condition.
Related to the first question, the second question has brought up some results which in deed should be fulfilled by the enterprise in the near future in order to re-study their situation.

6.3 Future Work

The restudy of the situation of InterAdria can be considered as a future challenge which would lead to new investigations on how the proposed changes have reflected and was it worth to study the situation in relation to OCTAVE-SM and quality levels stated in section 3.
7 References


CERT “Enterprise security” http://www.cert.org/octave (accessed: 08/04/02)


Tulane University, “information security at Tulane” http://security.tulane.edu/security-strategy.htm#_Toc112231456(accessed: 08/03/24)


Appendix A

Interviews

Below is presented the first interview prepared for the business runners of “InterAdria”.

Interview 1: CEO of “InterAdria”.

Organizational level

Q1. Considering the transit period in which your country is going through, can you tell how productive and organized is your enterprise in these circumstances and is your customer getting what you expect is the best?

Q1 – Answer: The situation in which our people are passing through is still critical even if there has been some changes for the best of the population. The transit period is not very formal, we try to follow the modern world in industry in economics and in academic life.

In our enterprise in which we have more than 100 employees we develop and we customize all our products for the best of the customer. Our product portfolio consists of several in-house-built products which are very advanced and can be comparable to even some of the most well-known companies in the world. Our business consists of several departments in which the software development and telecommunication department lead the business, by combining the latest technology and the latest developments of our skilled and professional staff members.

Currently our focus is at the customer and we try to give our best for them, therefore we think that each customer that worked with us is quite satisfied considering our well integrated and well developed products and our enterprise tactics.

Q2. Can you describe your main services that you provide in your enterprise, how different they are; how did you divide your personnel (is it only based on skills) and how did you group your assets, those that are in-house-build and which are bought for your premises?

Q2 – Answer: Our main and most advanced services are:
1. Software – development, integration, customization and upgrade.
2. Telecommunication – installation, configuration and implementation.
4. Construction work – site construction, turn-key solutions.
5. Education – trainings for different software solutions.

Our employees are divided mostly based on skills they have. Each department has different skilled people in the area they work.

As for assets, we have divided them in groups and for each department there are a number of assets available for our employees and a number of assets that are owned by the enterprise. This is the
main division. Our assets then are divided in sub groups: those that are developed or created in our enterprise and those that are bought and are ready to be deployed somewhere else.

Q3. Related to Security, how do you practice it and is there any proper security performance that is strong enough to protect yours assets, your people and your enterprise in general?

Q3 – Answer: Until now we have been partly satisfied with our security performance concerning this issue. Although we have had some dissatisfactions because there have been some internal and external threats. The issue of protection is very sensitive in our case, we try to protect all of our assets by including security strategies such cameras, fire alarms, alarm systems, but we still are not satisfied because there are other ways that intruders might have access that in our case this is the most dangerous attack which can happen specifically for our software assets. As for our employees this situation is also related to the current situation in the country, for which we think now its very calm and is passing through the tranzit steps towards the modern society.

Q4. Taking in consideration that your enterprise runs one of the most delicate businesses such as Software Development and knowing that these services and these assets are of the high importance for you, how critical they are in the current position, can they get easily exposed to unauthorized people because of the security issue or do you think they can be interrupted or distroyed violently?

Q4 – Answer: This is a good question. In deed we run one of the most interesting and sensitive business especially when it comes to our software development department. Our services include all of our products for which we have a fear that they might get unwantedly exposed to unauthorized persons. For this matter, we try to keep our products safe by not giving access directly to them through network, but then the fear of internal threat is also not neglected, because our employees come from different cultures and we can never guess or expect how would any of them behave in any case, would they act violently towards us – our enterprise/products, would they destroy them purposely or would they steal them!

I think that the current security status of our products is in a critical situation which we need to solve fastly especially for the internal threat, since the outer threat I think is reduced by using advanced security technologies for the network.

Q5: Does your enterprise have a strategic plan of protection, how well-organized do you think it is, and do you plan to progress in this aspect by doing new trainings and updates?

Q5 – Answer: There is a strategy and an organized way to deal with security. This is not very well invovled in our system, because we need to generate a more flexible –understandable system that could be easily absorbed by everyone.

Q6: Does your enterprise have well-formulated and well documented security policies which should be known to each employee, especially to those who have the role in the security area?

Q6 – Answer: Each person that have signed and agreed the contract form (this is for the internal issues within the enterprise), has read and agreed to all rules that are described one by one in the contract form. I think they are well-documented and oganized according to the laws of our region.

Organizational level/Information level

Q7: Is your enterprise well-prepared using the strategy of securing assets and any information? Today Directory Sercive is everywhere, and it shows the first security process accessing information and assets (software). Is your enterprise aware of this kind of database security strategy and do you practice such implementations and strategies?

Q7 – Answer: Yes we are prepared, but I can not say that we are well-prepared. In point of fact we use the product of Microsoft Active Directory which is very helpful, this kind of database is more present in the software development department, therefore for the near future we plan to implement
it to every employee / department by controlling the entire access of our private network so we are more sure of what is really happening throughout our enterprise.

Infrastructure level/ physical level

Q8: Your enterprise owns a number of valuable assets specifically those of the Software Development Department and the Telecommunication Department. Are you aware of what may affect negatively these assets considering that today the cyber space (network threats) is present 24/7 and that even natural disasters can not be predicted. Did you plan or organize any form of securing your premises from these damages?

**Q8 – Answer:** We are quite aware of all threats, but we think that such threats are present everywhere especially in our country and in the Balkan Peninsula. We try to control everything however we can, but in some cases this control is not enough and we see risk for many reasons. The risk is specifically present for our valuable software assets, which for us are some of the most important together with telecommunication assets which sometimes cost a lot of money. For natural disasters we are afraid when it comes to fire and water, but for big natural disasters such as volcano, tornado or hurricanes we are not aware of what might happen considering that our geographical position does not go through these kind of disasters.

Infrastructure level/ workflow level

Q9: Do you organize your infrastructure in a way that there is a predefined way of accessing your assets? Are there any steps that should be followed reaching the destination (ex. access specific information)?

**Q9 – Answer:** Actually we haven’t created a plan how to access our assets. In fact now we have a routine how we do that, which is not very good but we think that in the future there will be a formal plan.

Infrastructure level

Q10: Did you divide the responsibility for protecting and maintaining your assets?

**Q10 – Answer:** Yes of course. Each employee has its own responsibility, currently we have 4 people who take care of security issues in our enterprise. Some are responsible for the network, some for the mail server, another one for the database server.

Q11: How do you measure risk in your enterprise? Do you approximately know how risky might be just to think of some circumstances in which your assets could take place?

**Q11 – Answer:** Hmmm. This is very tricky. We have had many meetings concerning this issue. We have had meeting with our Board of Directors and we have had meetings with our Security Personnel.

The situation in which our asset or employees can appear is very unpredictable therefore we try to measure the risk by categorizing the risks, starting from the lower to the most dangerous risks.

Organizational level/workflow level

Q12: Knowing that you run this business for 20 years until now, are you aware of how many times your enterprise including people and assets are at risk? Can you give a qualitative measure in accordance with occurrence of example how often a threat can happen?

**Q12 – Answer:** The risk is always present, I can even say that everyday there is a risk for something, this is a normal process which happens everywhere and at anytime, so we try to avoid it but we can never be sure 100% that it won’t happen.

Q13 Do you create plans for your critical or for the most important/delicate assets? If yes, how do you generate plans and do you practice this frequently or at least when a new asset is developed or added to your valuable asset list?
Q13 – Answer: We haven’t created a formal plan for groups of assets individually, instead we have discussed and formed a general plan for all assets how should they be maintained and protected. For the delicate assets which are enterprise’s most important assets there is always a higher risk and more concern how to deal with them.

The general plan is pretty well organized, but is not balanced for the high and low importance assets, so I think that our enterprise is in progress to following up new discussions for a new strategy especially for security reasons.

Organizational level/infrastructure level

Q14: Do you know the main actors in the threatening process towards your enterprise? Can you list some of them by putting them in order starting from the most dangerous and delicate threat?

Q14 – Answer: Threat from any outside or inside factor is dangerous. What we have discussed and we have put it in the list with high and low risk category is as follows:

Inside threats:
1. An employee harming the system purposely
2. An employee stealing a valuable asset
3. An employee damaging the network and missusing the database system

Outside threats:
1. Crackers breaking into our network and missusing our data
2. Stealing our software assets
3. Breaking into our e-mail system / database system
4. Stealing our telecommunication devices from our enterprise facilities
5. Stealing our telecommunication devices from sites (construction fields)

Natural Disasters:
1. Water
2. Fire
3. Road Accidents

Workflow level

Q15. Risk Analysis is an important matter. Can you provide more details how do you take decisions when you analyze the risk list available, which is always present and any of them can happen at any time concerning the protection of your valuable assets? Do you think of any side-affects such as: reputation, financial, productivity or even fines?

Q15 – Answer: Decision making is an important and very crucial process. Sometimes you have to risk in order to get something good. Risk is always a reason that you have to take in consideration when you are deciding for something. We usually see risk when we apply for different tenders by giving low or high prices which in many cases is the key to decide who wins. In security this is different but again we think that sometimes we need to risk if needed in order to follow easy steps for our development of our products. This risk includes for example a program currently being developed which needs to be online for our employee purposes, which in fact is not good at all, since an online product can be exposed to intruders much easier than getting it out of the online network.

Q16. About your future plans? Do you think there is a need to upgrade your security strategy frequently by maybe investing in the latest technology including hardware and software and do you plan to refresh your personnel by giving extra trainings or even employing new skilled members that should deal with such activities?

Q16 – Answer: Future plans are always in target. Since with future plans we see the future developments, we always take new steps that until now have shown great success. For security and
for our hardware and software systems, we always follow the latest technologies without any problem. Our staff is also very well prepared for any technology, so whenever a new training is available we send them and we train them so they also get quite a good knowledge related to the security issue which de facto is always needed no matter what technology or product you use or work on it.

Appendix B

Interview 2: CIO of “InterAdria”.

Organizational level

Q1. Considering the transit period in which your country is going through, can you tell how productive and organized is your enterprise in these circumstances and is your customer getting what you expect is the best?

Q1 – Answer: As Chief Information Officer at InterAdria I have seen many positive willings first by our management and directorate and second by all our employees. What we try to sell is always give the best quality to our customers so we can make them happy. As an enterprise running in this country which in fact is not very developed, we provide very qualitative products which are well-known across our region and can be comparable to world-wide companies.

Q2. Can you describe your main services that you provide in your enterprise, how different they are; how did you divide your personnel (is it only based on skills) and how did you group your assets, those that are in-house-build and which are bought for your premises?

Q2 – Answer: Our focus is at the latest technology. We always are present in the best known world markets so we get well informed for everything. Therefore our focus is at software development services and telecommunication – radio communication services.

Q3. Related to Security, how do you practice it and is there any proper security performance that is strong enough to protect yours assets, your people and your enterprise in general?

Q3 – Answer: I consider security as the most important issue in our enterprise, this is because having a good security in a way releases us from the stress and fear that we have. So I can say that we have a good performance in the security issue which uses some of the latest technology to protect information / virtual assets and physical assets as well as personnel.

Q4. Taking in consideration that your enterprise runs one of the most delicate businesses such as Software Development and knowing that these services and these assets are of the high importance for you, how critical they are in the current position, can they get easily exposed to unauthorized people because of the security issue or do you think they can be interrupted or destroyed violently?

Q4 – Answer: Yes, in deed we are one of the most well known companies of our region for running this business, I can say that this kind of business is pretty hard to run since it requires a well qualified staff and a good enterprise for development, security and services. Therefore we try to avoid unauthorized access to any of our premises, I personally try to inform and try to talk to my colleagues of IT in order to remind them that they should be aware at every second of what they are doing and how often they check and control the connections.

Q5: Does your enterprise have a strategic plan of protection, how well-organized do you think it is, and do you plan to progress in this aspect by doing new trainings and updates?
Q5 – Answer: A strategic plan for security exists, every employee dealing with the security of any assets is aware of it. Although this strategy is a bit general, we hope that in the future we create a more specific strategic plan that can be appropriate for specific needs.

Q6: Does your enterprise have well-formulated and well documented security policies which should be known to each employee, especially to those who have the role in the security area?

Q6 – Answer: We have a lot of documentation, one of them is available for each employee who should be aware of all the actions that is ready to take. I think this has been quite helpful so far, but we try to provide more detailed documentations in the future that are specifically related to security strategy, their intimated information and even their developments.

Organizational level/Information level

Q7: Is your enterprise well-prepared using the strategy of securing assets and any information? Today Directory Service is everywhere, and it shows the first security process accessing information and assets (software). Is your enterprise aware of this kind of database security strategy and do you practice such implementations and strategies?

Q5 – Answer: In general we are quite prepared, we have often meetings specifically for this issue, and we ask our IT staff to present to us anything they need. I think they use quite strong database systems for access to the network (such as mail) and for other data (such as software) in order to keep them both secured.

Infrastructure level/ physical level

Q8: Your enterprise owns a number of valuable assets specifically those of the Software Development Department and the Telecommunication Department. Are you aware of what may affect negatively these assets considering that today the cyber space (network threats) is present 24/7 and that even natural disasters can not be predicted. Did you plan or organize any form of securing your premises from these damages?

Q8 – Answer: I’m pretty aware of attacks those that are from inside the enterprise and those that are from the outside. Running this business for such a long time, of course it gave you practice, because in a way we have tried everything and we know what can happen. Therefore we try to prepare rules for each employee and we try to give controls for every access at any time. For the unpredictable risks we are not so sure how to act, but we do backups pretty often sending this backup in a different place from the original one.

Infrastructure level/ workflow level

Q9: Do you organize your infrastructure in a way that there is a predefine way of accessing your assets? Are there any steps that should be followed reaching the destination (ex. access specific information)?

Q9 – Answer: Well, I can’t say that we have a specific plan or a predefined way of how to access specific information, but we know how to use it and which is the easiest way to do that. For this issues, we ask our IT to develope and to create security access controls every time someone wants to see belonging of the enterprise.

Infrastructure level

Q10: Did you divide the responsibility for protecting and maintaining your assets?
Q10 – Answer: Yes, we have groups of people who do their job according to their current position in our enterprise. Some work in cooperation with each other, some have an individual role, but in general cooperation is very much present and it functions very well.

Q11: How do you measure risk in your enterprise? Do you approximately know how risky might be just to think of some circumstances in which your assets could take place?

Q11 – Answer: Risk is always dangerous no matter how big it is. When the risk comes than we evaluate how much damage it can bring, so by measuring the damage of the risk than we decide how to act. Sometimes even to go through the risk is necessary in order to reach high success.

Organizational level/workflow level

Q12: Knowing that you run this business for 20 years until now, are you aware of how many times your enterprise including people and assets are at risk? Can you give a qualitative measure in accordance with occurrence of example how often a threat can happen?

Q12 – Answer: Risk is present everywhere. It can happen at any time in any moment. This kind of problem is present not just to our enterprise, but this is present to every enterprise which tries to reach success. Threats internal/external in our database and server systems are quite targeted therefore we try to take care of it by maintaining our system and getting our staff trained with high and the latest knowledge.

Q13 Do you create plans for you critical or for the most important/delicate assets? If yes, how do you generate plans and do you practice this frequently or at least when a new asset is developed or added to your valuable asset list?

Q13 – Answer: We don’t really create individual plans for levels of assets, but we have a strategic plan for all assets which we try to follow all the time, since until now it has been very helpful, even though we think of updating it.

Organizational level/infrastructure level

Q14: Do you know the main actors in the threatening process towards your enterprise? Can you list some of them by putting them in order starting from the most dangerous and delicate threat?

Q14 – Answer: There are quite a lot of threats. The most dangerous come from internal threats because I think that the easiest access to interrupt, destroy or even steal can happen when you are present for some time in the enterprise, and in a way you understand and you learn how to work with the systems that are deployed for the security reasons in the enterprise. External threats are threats that can happen at any time. In fact these are less dangerous than internal threats but are much more frequent, so they need a better care, especially to those threats that can destroy or steal your intimated data.

Workflow level

Q15. Risk Analysis is an important matter. Can you provide more details how do you take decisions when you analyze the risk list available, which is always present and any of them can happen at any time concerning the protection of your valuable assets? Do you think of any side-affects such as: reputation, financial, productivity or even fines?

Q15 – Answer: Well, sometimes we need to take decisions which are very risky, but when we think for the good of the enterprise we just have to do that. The risk list is quite long, there are pretty some different risks but we have to cope with that and sometimes accept it, even if it has maybe a big side-effect, but from all side-effects we try to avoid loosing our reputation, which for us is the most important.
Q16. About your future plans? Do you think there is a need to upgrade your security strategy frequently by maybe investing in the latest technology including hardware and software and do you plan to refresh your personnel by giving extra trainings or even employing new skilled members that should deal with such activities?

Q16 – Answers: We always think of future. For us future is everything, especially at the software development and education department, for which we try to prepare our staff with the latest technology who can easily be integrated in any development or training activity. Future for us means also a better security, since together with updates and trainings we get for our system and employees we also try to give some extra space to get trained for security reasons.

Appendix C

Interview 2 – Head of Software Development Department (Software Engineer) and Head of Software Projects (Software Engineer). This interview consists also two other answers from two software developers.

Interviewer number 1- software engineer
Q1: As software engineer of InterAdria, do you think that the current security strategy and the current infrastructure for your IT purposes has enough capacity for your needs? How do you contribute?
Q1- Answer: Well as an employee in InterAdria I think that there is a good infrastructure for the purpose of IT but I think that there is a lack of support regarding the security strategy and InterAdria needs to be developed further towards this direction to cover the capacity of employee needs.

Q2: As a staff of IT sector, is it hard to identify all needs of the enterprise in the aspect of technology and are you able to scan and see every movement what happens between all internal and external communication processes?
Q2- No Answer

Q3: In case a security threat (internally and externally) happens are you aware on how to react at that moment?
Q3- Answer: We don’t have a security policy yet and don’t know how to react in the proper and the right way but we sure do the best and react very fast upon the threat.

Q4: As IT personnel you always have the responsibility to take care of all virtual assets especially those that are in-house built such as software products. Are you able to track the movement and access to these assets between your colleagues? Do you think that there is always a very high potential risk that can happen at any time?
Q4- Answer: Yes the risk can happen if someone has the intention to harm a particular asset. The access and the movement of the software products can be tracked quite easily. And to prevent this InterAdria needs to come up with a good security strategy.

Q5: Do you have any strategically plan for the security of all or specific assets? Are you aware and well-prepared with advanced technologies that today affect positively? Can you mention some of these security technologies you use?
Q5 – Answer: I can say there is no strategic plan for security whatsoever; however the plan towards building a security strategy is under development. As for the security technologies we are familiar with Active directory which gives us a good overview of all accesses to our server and to each client

Q6: You probably see many viruses/spyware and other intruders that try to harm your network, database or the entire system of InterAdria. How do you react when it comes to valuable information or data that should not be exposed to anyone? This is related not only to your department, but this has also to do with financial data.
Q6 –Answer: for this we have an anti-virus Kaspersky 6.0.1.411 installed in each computer in the whole enterprise.

Q7: Can you be more specific for telling and describing the technology you use for the security of your database, for security of the mail server, web-site server, public data for the enterprise purposes and intimated data of employees?)?

Q8: What is your exact role at InterAdria. Do you cooperate with your colleagues for this role, or you have full responsibility? Please specify your position at this stage.
Q8 –Answer: My role in InterAdria is a Software Developer. I can say that in InterAdria it is more of a team work rather than a full responsibility (alone) work. So this means that we exchange ideas and work with other software developers in daily basis.

Q9: Taking in consideration your position for the protection and security strategy, do you think that there are times when you are not able to protect anything and that even by seeing that something might happen you cannot help? If yes, please specify the reasons why is this so, and how do you think you and the enterprise can solve it?
Q9 –Answer: As i stated above my responsibility has nothing to do with security strategy however if i can detect that anything will go wrong i will immediately act upon the threat by either letting the CIO know where and when the threat happened or i will try my best to help in every circumstance.

Q10: Since when you have been employed in this enterprise, do you like the strategy they use for advising you as an employee how to act and how to work? What would you change, and is there a need to change hardware or software for security reasons?
Q10 –Answer: My relations with the colleagues so far have been really good. I can say that not all the companies have this kind of so called “freedom”. I’m referring to it as a freedom since there is no formality between the colleagues and i wouldn’t change a thing about that. As for the hardware and software InterAdria is equipped with the latest advanced and trendy technology.

Q11: There are internal and external threats to you system? Can you please list them by giving priority to those that you think are the most dangerous and that need a fast change?
Q11 –Answer: Yes, i can say that InterAdria struggled in the past with some internal threats. And for this i think the most dangerous assets would be internal threats towards software, physical threats, outside threats upon software, etc.

Q12: Do you have any documentation and a strategic plan that you can easily read and follow the predefined rules so it eases your everyday tough job?
Q12 –Answer: As i stated above InterAdria has no security policy whatsoever but i think they are working on this and i think it will be implemented in the near future.

Q13: There are probably many cases when you are the responsible person to decide if you need to take a specific action or not. In many cases this can be risky, how do you compare and prepare the list of advantages and disadvantaf if you need to take an action that might be risky (loose data, destroy hardware or something similar)?
Q13 –Answer: I don’t have the permission to take any actions without first talking with the CIO, but there can be people who can act without having the permission so this can be a disadvantage since no one will know if the “employee” have a bad intention towards some assets because right now InterAdria relies on the trust of their employees which i personally think its not that reliable nowadays.

Q14: Did you by your own divided all valuable assets, so you know where you need to act immediately, is your technology of security able to perform fast and how did you configure or program it?
Q14- No Answer

Q15: Do you run your job through a security policy, do you strictly follow if your enterprise has one, or sometimes you need to act your own way?
Q15 –Answer: we dont have any security policy but we are always in touch with the CIO however we sometimes can act on our own way even though this happened rarely.
Q16: IT future is always in mind. An IT person always thinks of the latest technologies especially for hardware and security software. How often does your enterprise invest in this area, is this enough for your needs?
Q16 –Answer I state it once and i will say it again, InterAdria is equipped with a quite trendy technology. We as software developers don’t need an update on hardware every year but we are updated with the latest software. The Hardware is one of the newest and so far didn’t have any problems regarding our work.

Appendix D
Interviewer number 2- software engineer

Q1: As software engineer of InterAdria, do you think that the current security strategy and the current infrastructure for your IT purposes has enough capacity for your needs? How do you contribute?
Q1: Answer – Technology is always one of the main conditions that tell how you function in an enterprise, specifically an IT enterprise. To say the truth, today technology is being developed very fast so we need to follow the latest developments and infrastructures in order to be in a good position compared to our competitors.
Currently we use some of the latest technologies for our servers and our software products. Soon we except to get the latest produced HP Server which will be better in performance and of course in security. This new server will fulfill all the gaps that exist and will ease our everyday work.
As a software engineer I work with software but my second position is to contribute to checking the communication in our local network and with the outside world. My duty is also to take care of our web server mail server.

Q2: as a staff of IT sector is it hard to identify all needs of the enterprise in the aspect of technology and are you able to scan and see every movement what happens between all internal and external communication processes?
Q2: Answer – It’s not very hard to identify the needs of our enterprise. In point of fact the cooperation between us (colleagues) works pretty well, so we combine all our ideas when we see that something is missing or needs to be replaced.
Sometimes it’s quite hard to follow everything, it happened that once we were misused by our own colleagues and of course it happened to be attacked by many external factors (viruses, spywares, crackers....).
I think this issue is quite delicate and these things happen everywhere, but now we are a very strong team and we have a stronger infrastructure.

Q3: In case a security threat (internally and externally) happens are you aware on how to react at that moment?
Q3: Answer – Yes we are pretty aware, we usually act very fast, before it’s too late. Sometimes it’s not very easy to detect everything at the moment, but it doesn’t go to long until we monitor what happened so we know how to proceed.

Q4: As IT personnel you always have the responsibility to take care of all virtual assets especially those that are in-house built such as software products. Are you able to track the movement and access to these assets between your colleagues? Do you think that there is always a very high potential risk that can happen at any time?
Q4: Answer – Our assets ”Software” that today represent the most valuable assets of our enterprise are very secured and they are saved in special offline disks and are available only by request to our Software Manager. How we organize our development now is a bit different. We never give the complete solution to our software developers, but we give some parts of it based on some requirements that need to be developed. This seems to lead us to a better security strategy in the future.
Working with Software and being the responsible person for it, its pretty risky, although now, the way we have organized the approach to any software solution, seems to be functioning very well.
Q5: Do you have any strategically plan for the security of all or specific assets? Are you aware and well-prepared with advanced technologies that today affect positively? Can you mention some of these security technologies you use?
Q5- Answer: I already mentioned in the previous answer how we have organized the way of using and approaching our software systems. This strategy or I can say this plan is leading us to successfully managing our department. Each software requires a username and password in order to open a solution, its the same procedure if anyone needs to access our web server or mail server. In fact there are a lot of improvements that need to be done in the future, but currently I think that we are progressing very well.

Q6: You probably see many viruses/spyware and other intruders that try to harm your network, database or the entire system of InterAdria. How do you react when it comes to valuable information or data that should not be exposed to anyone? This is related not only to your department, but this has also to do with financial data.
Q6: Answer – When I need to take care of the Network, I really need to concentrate and see what is happening or what has happened. It’s a pretty tough job when it comes to interventions that must be done quickly. Many times it’s more important to take care of the servers in case they are down rather than just checking viruses or spywares, since we have the antivirus and antispyware software’s and of course the firewall that do most of the job for us.

Q7: Can you be more specific for telling and describing the technology you use for the security of your database, for security of the mail server, web-site server, public data for the enterprise purposes and intimated data of employees?)?
Q7: - Answer – All of our databases currently run on MSSQL 2005. This is a quite strong database system with a good security. Each database requires a network connection by typing username and password. The database resides in the server which is not online for outside connections but only for our administrative and work purposes. Every information stored or used by our employees stays confidential. Data which are more delicate such as those of the financial and management department are stored in separate Hard Drives and are only available by responsible person who uses them. We are a bit worried about backups which need to be saved in a place different from the original, in case of any emergency exit such natural disasters.

Q8: What is your exact role at InterAdria. Do you cooperate with your colleagues for this role, or you have full responsibility? Please specify your position at this stage.
Q8: Answer – My title is Software Engineer and my primary duty is to develop the architecture of the software and database followed by documentation. I also am responsible to check servers time by time. For every software we do consulting with other team members so we know what to develop and who should work in specific parts of the project.

Q9: Taking in consideration you position for the protection and security strategy, do you think that there are times when you are not able to protect anything and that even by seeing that something might happen you cannot help? If yes, please specify the reasons why is this so, and how do you think you and the enterprise can solve it?
Q9: Answer – Whenever I feel that I’m not very productive or I can’t do anything in emergency cases I contact my colleagues and I ask for help, so we try to cooperate all the time, even though sometimes it’s a bit hard to explain the situation fast, but most of the times we overcome the situation very good.

Q10: since when you have been employed in this enterprise, do you like the strategy they use for advising you as an employee how to act and how to work? What would you change, and is there a need to change hardware or software for security reasons?
Q10: Answer – I work in this enterprise since 2005. Since then I have gained a very good knowledge by learning new things and improving my skills. I hope I have been contributing to this enterprise for good, and I wish that our future will always be bright as it is now. The strategy of the enterprise is being updated every month and every year with new good features which is for the best of the enterprise. We are also updating our software’s and we are very frequently buying new hardware.

Q11: There are internal and external threats to your system? Can you please list them by giving priority to those that you think are the most dangerous and that need a fast change?

Q11: Answer - It’s a bit hard to identify and to list them all at because the spectrum of these attacks is very huge that sometimes you don’t know what can happen. Some of the main factors that can be devastating are as the following:

- Viruses
- Crackers
- Thieves
- Irresponsible staff
- Natural Disasters

Q12: Do you have any documentation and a strategic plan that you can easily read and follow the predefined rules so it eases your everyday tough job?

Q12: Answer – There isn’t a strategic plan. Of course it would be much easier for us and for the enterprise to have one, so everyone knows the rules the program and everything else related to the everyday work. I hope that in the near future we design a plan for our needs which will be perfect and important to us.

Q13: There are probably many cases when you are the responsible person to decide if you need to take a specific action or not. In many cases this can be risky, how do you compare and prepare the list of advantages and disadvantage if you need to take an action that might be risky (loose data, destroy hardware or something similar)?

Q13: Answer – Yes, there are many times when I need to decide for an action. Thankfully, it still didn’t happen to be responsible for a risky action. I hope it won’t happen, since this is pretty tough to decide.

Q14: Did you by your own divided all valuable assets, so you know where you need to act immediately, is your technology of security able to perform fast and how did you configure or program it?

Q14: Answer – In our department every asset is valuable since we deal with software and databases. These valuable assets can be divided with a higher or a lower value, but all of them are secured using the same method. These assets are backup very frequently and whenever a new update is done, so we keep them in safe storages which are external and not online.

Q15: Do you run your job through a security policy, do you strictly follow if your enterprise has one, or sometimes you need to act your own way?

Q15: Answer – I already mentioned that there isn’t a strategic plan and neither it is a strict security policy which we should be aware of. Our management has decided to bring some new rules to the enterprise regarding security so we hope for the best.

Q16: IT future is always in mind. An IT person always thinks of the latest technologies especially for hardware and security software. How often does your enterprise invest in this area, is this enough for your needs?

Q16: Answer – Until now we didn’t really have the latest technology in our hands, from now on our colleagues and all of us are requesting new hardware and new software to have a better performance and a better quality, since this is a need for our enterprise, and luckily we have these deliveries very fast. Currently we have bought the latest Server Configuration and the latest Software Server which is not installed yet, but we think that the network performance will be increased and will work fast.
Appendix E

Answers Interviewer3- Head of Software Development Department (Software Engineer)

Q1: as software engineer of InterAdria, do you think that the current security strategy and the current infrastructure for your IT purposes has enough capacity for your needs? How do you contribute?
Q1-Answer: No it is not enough capacity for our needs. We planned to extend our capacities with new server for enterprise needs.

Q2: as a staff of IT sector is it hard to identify all needs of the enterprise in the aspect of technology and are you able to scan and see every movement what happens between all internal and external communication processes?
Q2-Answer: For me it is a bit difficult to identify all needs because in the market, now in very big spectrum of IT products, find and choice proper product for scanning and see all movement in internal and external communication processes.

Q3: In case a security threat (internally and externally) happens are you aware on how to react at that moment?
Q3-Answer: In this case and in this moment without proper tracking software, I am not in the position to react in proper way for this situation.

Q4: As IT personnel you always have the responsibility to take care of all virtual assets especially those that are in-house built such as software products. Are you able to track the movement and access to these assets between your colleagues? Do you think that there is always a very high potential risk that can happen at any time?
Q4-Answer: Colleagues with whom we work in software department, InterAdria has built a mutual trust regarding security, so we all do our best to function in the best way. While we are working for a better security solution for internal and external threats we are very careful on picking the colleagues in this.

Q5: Do you have any strategically plan for the security of all or specific assets? Are you aware and well-prepared with advanced technologies that today affect positively? Can you mention some of these security technologies you use?
Q5-Answer: As said we don’t have a strategic plan for our security and as we are working upon this issue we are waiting for the arrival of a new server and I hope that the strategic plan for security will be ready by then.

Q6: You probably see many viruses/spyware and other intruders that try to harm your network, database or the entire system of InterAdria. How do you react when it comes to valuable information or data that should not be exposed to anyone? This is related not only to your department, but this has also to do with financial data.
Q6-Answer: To secure our data, applications and different kinds of information from many viruses, spywares and other intruders that try to harm our network, we have installed Kaspersky Anti-Virus 6.0.1.411 version in all our computers in network.

Q7: Can you be more specific for telling and describing the technology you use for the security of your database, for security of the mail server, web-site server, public data for the enterprise purposes and intimated data of employees?)?
Q7-Answer: I stated above AntiVirus in Kaspersky 6.0.

Q8: What is your exact role at InterAdria. Do you cooperate with your colleagues for this role, or you have full responsibility? Please specify your position at this stage.
Q8-Answer: My role is to manage the work with the other companies which include organizing the work and taking care of how the software’s are developing. In my job it is very important to state the relations between colleagues and especially in software department.
Q9: Taking in consideration you position for the protection and security strategy, do you think that there are times when you are not able to protect anything and that even by seeing that something might happen you cannot help? If yes, please specify the reasons why is this so, and how do you think you and the enterprise can solve it?
Q9-Answer: Yes it is true. Sometime I see that something might happen and I cannot help! The reason is that we once were reliable on the trust of our colleague and the worst happen when an internal threat happened. I hope that till a new solution towards the security strategy is done we won’t experience the same threats as we once did.

Q10: since when you have been employed in this enterprise, do you like the strategy they use for advising you as an employee how to act and how to work? What would you change, and is there a need to change hardware or software for security reasons?
Q10-Answer: From my point of view, relationship between key personnel and developers in Software Department is built based on the mutual trust even though the installation of the new software and hardware is critique so this mutual trust must be very reliable.

Q11: There are internal and external threats to you system? Can you please list them by giving priority to those that you think are the most dangerous and that need a fast change ?
Q11. No Answer.

Q12: Do you have any documentation and a strategic plan that you can easily read and follow the predefined rules so it eases your everyday tough job?
Q12-Answer: No I don’t have any daily documentation or strategic plan

Q13: There are probably many cases when you are the responsible person to decide if you need to take a specific action or not. In many cases this can be risky, how do you compare and prepare the list of advantages and disadvantage if you need to take an action that might be risky (loose data, destroy hardware or something similar)?
Q13-Answer: Yes, this is true. In some cases I need to take action for risky situation like testing periods for project where we need to create backups for DB or developed application. When we need to do this, usually we need to be very careful for projects almost in the end phase of development or for live data bases.

Q14: Did you by your own divided all valuable assets, so you know where you need to act immediately, is your technology of security able to perform fast and how did you configure or program it?
Q14. No Answer.

Q15: Do you run your job through a security policy, do you strictly follow if your enterprise has one, or sometimes you need to act your own way?
Q15- Answer: I mentioned in previous question that we don’t have our security policy in enterprise. For this reason, we are acting in our own way.

Q16: IT future is always in mind. An IT person always thinks of the latest technologies especially for hardware and security software. How often does your enterprise invest in this area, is this enough for your needs?
Q16-Answer: as I mentioned above, in our plane is new investment on hardware and security software. After this step, our strategic planning will be to escort all new IT development in security field.