Proceedings of the International Multiconference on
Computer Science and Information Technology, pp. 485 – 497

ISSN 1896-7094

The OCTAVE methodology as a risk analysis tool for business resources

Pyka Marek, Januszkiewicz Paulina

Academy of Business in Dąbrowa Górnicza, Poland
mpyka@wsb.edu.pl, pjanuszkiewicz@wsb.edu.pl

Abstract. In this article the authors conduct a discussion concerning methodology that improves information management and protection decision making process. The authors describe OCTAVE (The Operationally Critical Threat, Asset, and Vulnerability Evaluation) using real-life examples and reference to the Polish legal regulations. The purpose of the article is to present a methodology, which is successfully being employed in Western-Europe countries and to show that it can also be efficiently conducted in Poland, fitting well into the policies of many companies.

1 Introduction

Nowadays, companies develop dynamically along with their computing infrastructure. It is common phenomenon that this development is not accompanied by any sort of strategy or cost evaluation for the expansion of the IT infrastructure. In constant aspiration to enlarge their assets, companies pay little attention to the issue of data protection. Constant flow of reports about various electronic crimes causing severe business losses shows how short-sighted such an approach proves to be. Thanks to such proceedings, executives of many companies are starting to be aware of the fact that information is currently the most precious commodity and that issues related to the computing infrastructure may influence the whole of the business process.

Unfamiliarity with the security market which often results form the desire to save funds, often leads to hasty implementation of widely advertised security solutions or to resorting to the services of poorly trained consultants. People often hope that buying the latest tool or piece of technology will solve their security problems. Few organizations stop to evaluate what they are actually trying to protect (and why) from an organizational perspective before selecting solutions. In our work in the field of information security, we have found that security issues tend to be complex and are rarely solved simply by applying a piece of technology. Most security issues are firmly rooted in one or more organizational and business issues. Before implementing security solutions, we should consider characterizing the true nature of the underlying problems by evaluating our security needs and risks in the context of business. Proper security solutions should economically protect the company and eliminate the unnecessary risk related to business activity. Proper cost and security efficiency evaluation should include resources that are to be protected, possible threats and losses, as well as expenses related to unpredictable events. It is important to remember that mixing security with functionality may prove to be very expensive. Perfectly secured resources become virtually useless, while a company that aims at highest functionality cannot be perfectly protected. Methodologies that improve the risk minimization process allow determining the level of balance. In such cases, the resource protection strategy should go together with the tendency to take a level of accepted risk („How Much Security Is Enough?" CERT group). Companies that commit themselves to conduct the described processes should assume the necessity of organizational and hardware changes. Only such approach to planning resource protection allows reaching the desired level of security. One should also perform periodical surveys of resources, threats and risk, as well as take account for

the changing conditions (higher level of threat, hardware failure etc.). In the majority of methodologies, a model approach is assumed ("In-depth Defense" – Figure 1) [13]. In-depth analysis of the company's architecture lowers the risk of a successful attack and, therefore, data loss. Failing to comply with proper security principles might bring severe business and legal effects.

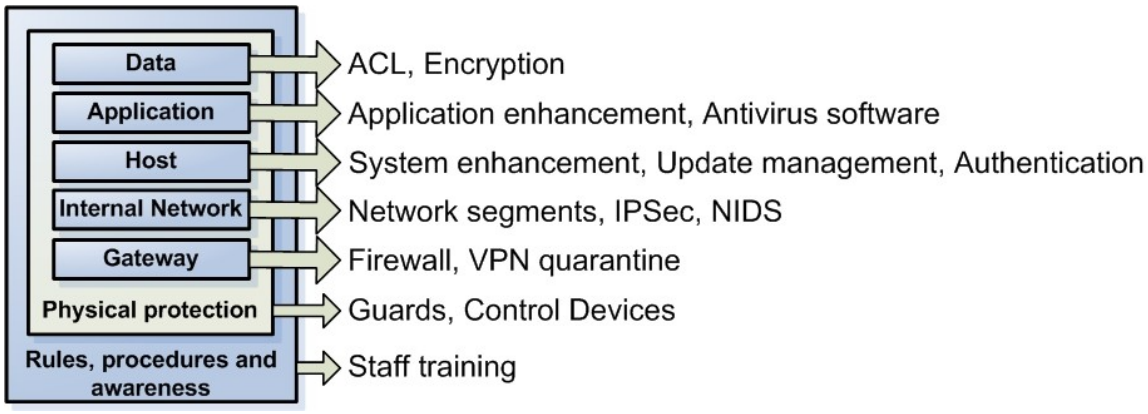

Fig. 1. „In-depth Defense" model [13].

Information can be divided into two categories: information that a company wants to protect and information that a company must protect. The Polish law forces organizations to protect various kinds of information. This mainly applies to personal data protection. Some companies must protect information, which is subject to additional legal acts: Ustawa o Ochronie Danych Osobowych—Personal Data Protection Act, Ustawa o Ochronie Informacji Niejawnych—Confidential Information Protection Act, Tajemnica Bankowa—Banking Confidentiality, Tajemnica Służbowa—Confidential Information. All employees have to comply with these regulations, which also force appropriate security measures, adapted to the particular kind of information that requires protection. Currently there are several dozens of information types in Poland – legal regulations force organizations to familiarize themselves with those acts, as well as to employ them properly in practice [4]. This is far from easy, considering the vast amount of various legal acts in Poland. Because of the varieties and limitations of current security evaluation methods, one may become confused when trying to select an appropriate method for evaluating information security risks. Most of the current methods are "bottom-up": they start with the computing infrastructure and focus on the technological vulnerabilities without considering the risks to the organization's mission and business objectives. A better alternative is to look at the organization itself and identify what needs to be protected, determine why it is at risk, and develop solutions requiring both technology- and practice-based solutions.

A comprehensive information security risk evaluation approach:

- Incorporates assets, threats, and vulnerabilities
- Enables decision makers to develop relative priorities based on what is important to the organization
- Incorporates organizational issues related to how people use the computing infrastructure to meet the business objectives of the organization
- Incorporates technological issues related to the configuration of the computing infrastructure
- Should be a flexible method that can be uniquely tailored to each organization

As the technological development proceeds, more and more complex data protection schemes arise. Because of this, many methodologies has been developed. Currently, one of the widespread information management policies is TISM (Total Information Security Management). This methodology helps to develop an appropriate implementation plan of information resources protection, based on binding legal acts, norms (PN ISO/IEC 17799:2003, PN-I-07799-2:2005) accepted standards and business principles of a given company. Thanks to this, a given company can establish proper security requirements for teleinformatic systems, as well as determine

the tasks and responsibility levels for particular individuals, who are admitted to the corporate secrets and to the management of critical systems. The implementation of TISM includes a theoretical part, when regulations, forms and other security documentation is created and a practical part, when penetration tests and audits are (LAN, Internet/LAN connection) conducted. This methodology is very time-consuming and requires large resources, this is the reason for Polish companies to seek an alternative procedure.

OCTAVE (Operationally Critical Threat , Asset and Vulnerability Evaluation) is a methodology that has not yet taken hold in Poland. An example of OCTAVE implementation, for small and medium companies, based on Polish law, shall be presented in this article.

2 The OCTAVE Method

2.1 An Introduction to the OCTAVE Method

One way to create a context-sensitive evaluation approach is to define a basic set of requirements for the evaluation and then develop a series, or family, of methods that meet those requirements. Each method within the approach could be targeted to a unique operational environment or situation.

OCTAVE is a methodology that improves the decision making process concerning protection and management of resources in a company. It was developed in year 2001 by the Carnegie Mellon University. Risk assessment is based on three basic principles of security administration: confidentiality, integrity, availability – by means of simple classification of critical information, one will receive a plan of protection for the given information. Authors conceived the OCTAVE project to define a systematic, organization-wide approach to evaluating information security risks comprising multiple methods consistent with the approach. The OCTAVE methodology designed the approach to be self-directed, enabling people to learn about security issues and improve their organization's security posture without unnecessary reliance on outside experts and vendors. An evaluation by itself only provides a direction for an organization's information security activities. Meaningful improvement will not occur unless the organization follows through by implementing the results of the evaluation and managing its information security risks. OCTAVE is an important first step in approaching information security risk management. The OCTAVE approach is defined in a set of criteria that includes principles, attributes, and outputs. Principles are the fundamental concepts driving the nature of the evaluation. They define the philosophy that shapes the evaluation process. For example, self-direction is one of the principles of OCTAVE. The concept of self-direction means that people inside the organization are in the best position to lead the evaluation and make decisions. The requirements of the evaluation are embodied in the attributes and outputs. Attributes are the distinctive qualities, or characteristics, of the evaluation. They are the requirements that define the basic elements of the OCTAVE approach and define what is necessary to make the evaluation a success from both the process and organizational perspectives. Attributes are derived from the OCTAVE principles. For example, one of the attributes of OCTAVE is that an interdisciplinary team (the analysis team) staffed by personnel from the organization leads the evaluation. The principle behind the creation of an analysis team is self-direction. Finally, outputs define the outcomes that an analysis team must achieve during the evaluation. Table 1 lists the structure of the principles, attributes, and outputs that we will examine in this chapter. We begin our exploration of the OCTAVE approach in the next section by looking at principles.

OCTAVE is about organizing appropriate workshops in a company. During those workshops, the employees themselves make the decisions concerning the level of importance for particular data resources. In order to make the best decision possible, it is necessary to attribute threat categories to particular resources. By resources we mean information as well as systems that process the information (along with supplementary applications), the company employees themselves are also considered a resource. In OCTAVE, threats are described by three logical structures – a threat profile is created by proper reference to those structures. Thanks to this, the OCTAVE implementation team is able to determine the threat range for the given resources. If the team deter-

mines the level of risk and understands the potential damage due to data loss, it will be able to take proper steps to minimize it and ensure better protection of the organization's resources.

Tab. 1. Information Security Principles, Attributes, and Outputs.

Information Security Principles, Attributes, and Outputs		
Principles	**Attributes**	
Self-direction Adaptable measures Defined process Foundation for a continuous process Foward-looking view Focus on the critical few Integrated Management Open communication Global perspective Teamwork	Analysis team and augmenting analysis team skills Catalog of practices Generic threat profile Catalog of vulnerabilities Defined evaluation activities Documented evaluation results Evaluation scope and next steps Focus on risk and focused activities Organizational and technological issues Business and information technology participation Senior management participation and collaborative approach	
Outputs		
Phase 1	**Phase 2**	**Phase 3**
Critical assets Security requirements for critical assets Threats to critical assets Current security practices Current organizational vulnerabilities	Key components Current technology vulnerabilities	Risks to critical assets Risk measures Protection strategy Risk mitigation plans

2.2 Characteristics of OCTAVE

The OCTAVE methodology is interesting, because it is perfectly adjusted to the policies of many companies. Every company has information that requires protection. Mere knowledge of the risks will not protect our business. OCTAVE should be applied regularly, because in large companies, the flow of information is constant. It is common for some given data to gain more importance over time. The lack of regularity may lead to data compromise or legal consequences. OCTAVE is a time consuming process, however, it should not be neglected. For organizational purposes, it is divided into three phases [5]:

Phase 1: Build Asset-Based Threat Profiles – it involves the evaluation of the company's security strategy and the determination of possessed resources. During this phase, the employees should be aware of the resources possessed by the company and which of them require special protection. Security requirements for this type of resources should be determined. The employees describe the security measures applied by the company so far and attempt to determine weaknesses in this strategy. This phase involves gathering introductory information; it is mainly based on the interviews with the employees. Phase 1 makes the staff aware of the importance of data protection, as well as describes the potential losses that could emerge in case of a vital data loss.

Phase 2: Identify Infrastructure Vulnerabilities – involves the evaluation of the information management system. It is mainly based on the data gathered during Phase 1. Data protection vulnerabilities are being surveyed with focus on technological issues. Key issues for the future strategy are being determined. This phase involves gathering data from the employees of the IT department, executives and other staff. A common solution should be developed, without hindering the present business model of the company.

Phase 3: Develop Security Strategy and Plans – this is the phase of risk analysis. Information gathered in Phase 1 and Phase 2 are used to assess the risk of data compromise in the company and the risk associated with the company's business activity. The security strategy and ways of minimizing the risk of data loss are being developed. With the exact information concerning the business model of the company, we are able to determine the attack types, which might take place in the future. In phase 3, the exact procedures are being created. The team that conducts the OCTAVE process must verify the legal status of the guidelines.

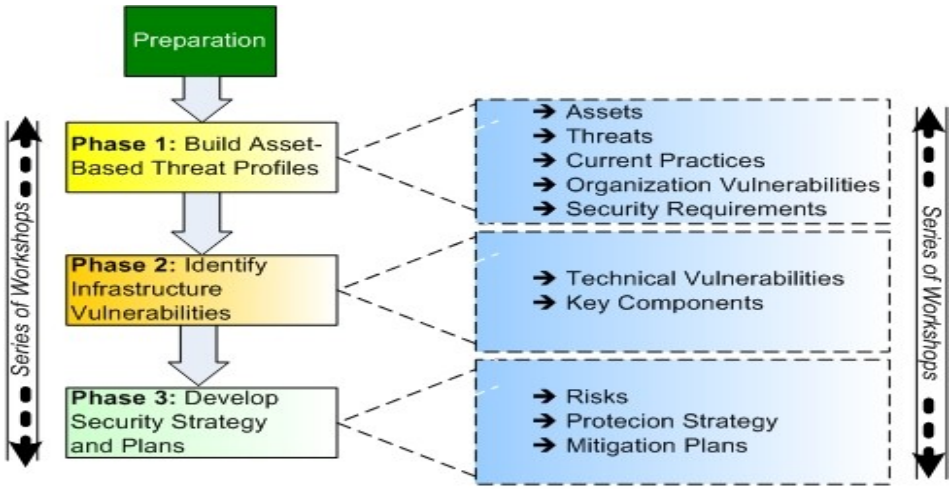

Fig. 2. The division of the OCTAVE process with sub-processes.

The line of business of the given organization plays a key role in the final decisions concerning data management strategy. OCTAVE assumes that the level of risk tolerance for a given company should be determined first. The security strategy should be developed later, in order to ensure the highest possible level of protection, without hindering business activities. Issues taken into consideration are: legal limitations, expenses of implementing the new strategy, productivity and security of consumer data. The documentation of OCTAVE methodology is very extensive, which ensures detailed data verification. However, an in-depth analysis of resources is not always necessary. For such cases, OCTAVE-S has been developed. It is used in small or medium-sized companies (employing not more than 100 people). The differences between those processes are visible during the conduction of workshops for the employees. Only several people are needed to perform the risk analysis. It is said that OCTAVE-S is a much easier solution. However, the choice of the variant depends only on the needs of an organization. There are companies, where both OCTAVE and OCTAVE-S would turn out to be a good solution – in such cases an initial calculation may prove to be helpful in determining the optimal methodology. The conduction of both processes takes about 3 days of time. However, when developing a strategy with the aid of OCTAVE, one must consider the budget available for this purpose.

If the OCTAVE methodology is to bring the intended results, the company must be aware of the threats that might occur for the possessed resources. Figure 3 illustrates the results of a survey conducted by CERT Polska in 2005 [10]. *Attack on information security* takes up only 0,2 % of all threats, while *Information gathering* goes as high as 51,9%. From the same report one can learn that commercial companies are the most common victims of attacks (53,1%). It is easy to draw a conclusion that the probability of *Information gathering* taking place in a company, is rising proportionally with the size of the company and the amount of information possessed by it. CERT Polska noted 2516 of such incidents in 2005, however, this is only the number of officially reported cases. Such statistics should make companies aware of the importance of protecting their resources. The OCTAVE methodology is very elastic in implementation. Basing on such reports, one can rule out the most likely threats and focus on finding solutions to the less common ones.

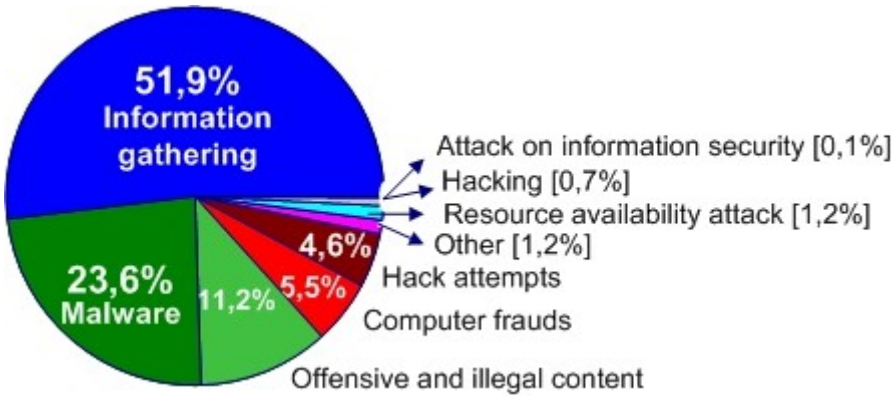

Fig. 3. Typical Threat Frequency in 2005. [Source: CERT Polska—Annual Report 2005]

2.3 Threats and Security Measures in OCTAVE

OCTAVE takes into consideration threats illustrated on Figure 4.

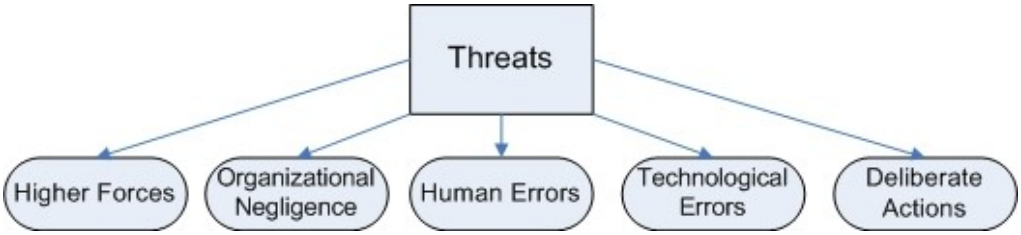

Fig. 4. The division of existing threats – Federal Office for Information Technology Security (BSI) [8].

Higher forces are threats, for which one can prepare but cannot directly influence them (for example fire, flood, network failure). The described methodology should minimize the risk resulting from improperly organized data processing (Organizational Negligence). Threats associated with this issue are, for example, unauthorized access to resources, privilege escalation or lack of resource control – these are the most commonly omitted aspects of security in many organizations. Human errors are also highly important, they make over 70% of threats. Workshops offered by OCTAVE also make the staff more aware of various threats. Technological errors may sometimes directly result from deliberate actions. Deliberately causing a network failure becomes a technological error and a direct trouble for the company. Dishonest staff or external attacks are usually taken into consideration in a later stage.

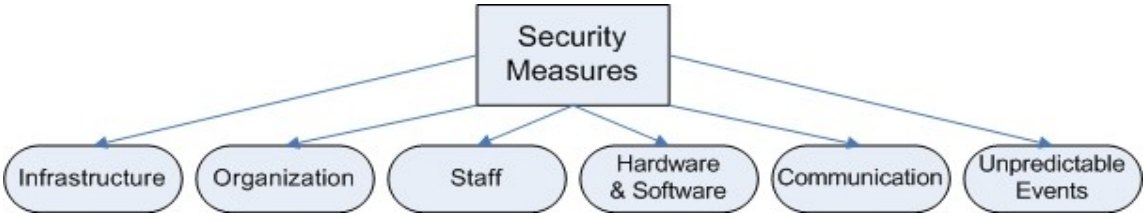

Fig. 5. The logical division of security measures in the OCTAVE process [8].

In response to the threats defined in the preliminary phase, OCTAVE also includes proposing certain solutions, in order to minimize the likelihood of those threats to occur. Security solutions for threats named in Figure 5 are being considered. Those are general assumptions; however, drawing up details for them might result in a very good starting point for resource protection. The security of a company involves various factors, which are directly adapted to business purposes or attack susceptibility. The conduction of OCTAVE methodology allows us to notice certain details, which may help to determine those factors. Let us remember that there is no such thing as perfect security. There is no plan in existence that would eliminate all risks. There are threats which we are unable to predict. However, OCTAVE is not used to create emergency plans for such cases; it is a methodology that helps to determine the risk, not to counteract existing threats.

OCTAVE is useful in preventing losses, not in repairing damage. One can only calculate the risk of a given event to occur – this is performed thanks to information gathered during phases 1 & 2. Emergency plans are being developed, which are to be applied in case of an unpredicted event. The security improvement strategy based on the OCTAVE methodology is a good guideline for a company and its employees – it tells them what to do, in order to minimize the risk of losses. Thanks to this, the company gains a reputation of being trustworthy and learns how to manage information security.

3 OCTAVE Workshops

The OCTAVE Method involves two types of workshops: (1) facilitated discussions with various members of the organization and (2) workshops in which the analysis team conducts a series of activities on its own. All workshops have a leader and a scribe. The leader is responsible for guiding all workshop activities and ensuring that all of these (including preparatory and follow-up activities) are completed. The leader is also responsible for ensuring that all participants understand their roles and that any new or supplementary analysis team members are ready to participate actively in the workshop. All workshop leaders should also make sure that they select a decision-making approach (e.g., majority vote, consensus) to be used during the workshops. Scribes are responsible for recording information generated during the workshops, either electronically or on paper. Please note that you might not have the same leader or scribe for all workshops.

3.1 Preparation

The initial focus of the OCTAVE Method is preparing for the evaluation. We have found the following to be key success factors [6]:

- Getting senior management sponsorship. This is the top success factor for information security risk evaluations. If senior managers do not support the process, staff support for the evaluation will dissipate quickly.
- Selecting the analysis team. The analysis team is responsible for managing the process and analyzing information. The members of the team need to have sufficient skills and training to lead the evaluation and to know when to augment their knowledge and skills by including additional people for one or more activities.
- Setting the appropriate scope of the OCTAVE Method. The evaluation should include important operational areas, but the scope cannot get too big. If it is too broad, it will be difficult for the analysis team to analyze all of the information. If the scope of the evaluation is too small, the results may not be as meaningful as they should be.
- Selecting participants. During the knowledge elicitation workshops (processes 1 to 3), staff members from multiple organizational levels will contribute their knowledge about the organization. They should be assigned to workshops because of their knowledge and skills, not solely based on who is available.

The goal of preparation is to make sure that the evaluation is scoped properly, that the organization's senior managers support it, and that everyone participating in the process understands his or her role.

3.2 Phase 1: Build Asset-Based Threat Profiles

In phase 1 you begin to build the organizational view of OCTAVE by focusing on the people in the organization. Figure 6 illustrates the four processes in phase 1.

Processes 1 to 3. The analysis team facilitates knowledge elicitation workshops during processes 1 to 3. Participants from across the organization contribute their unique perspectives about what is important to the organization (assets) and how well those assets are being protected. The following list highlights the audience for each of the processes:

- Process 1: Identify Senior Management Knowledge. The participants in this process are the organization's senior managers.
- Process 2: Identify Operational Area Management Knowledge. The participants in this process are the organization's operational area (middle) managers.
- Process 3: Identify Staff Knowledge. The participants in this process are the organization's staff members. Information technology staff members normally participate in a separate workshop from the one attended by general staff members.

Four activities are undertaken to elicit knowledge from workshop participants during processes 1 to 3 . This is the identification of: assets, relative priorities, areas of concern, security requirements for the most important assets and capture of knowledge of current security practices and organizational vulnerabilities.

Process 4: Create Threat Profiles. The participants in this process are the analysis team members. During process 4, the team identifies the assets that are most critical to the organization and describes how those assets are threatened. Process 4 comprises the following activities : consolidating information from processes 1 to 3, selecting critical assets, refining security requirements for critical assets, identifying threats to critical assets.

3.3 Phase 2: Identify Infrastructure Vulnerabilities

Phase 2 is also called the "technological view" of the OCTAVE Method, because this is where you turn your attention to your organization's computing infrastructure. The second phase of the evaluation includes two processes, depicted in Figure 7.

Process 5: Identify Key Components. The participants in this process are the analysis team and selected members of the information technology (IT) staff. The ultimate objective of process 5 is to select infrastructure components to be examined for technological weaknesses during process 6. Process 5 consists of two activities: identifying key classes of components and identifying infrastructure components to be examined.

Process 6: Evaluate Selected Components. The participants in this process are the analysis team and selected members of the IT staff. The goal of process 6 is to identify technological weaknesses in the infrastructure components that were identified during process 5. The technological weaknesses provide an indication of how vulnerable the organization's computing infrastructure is. Process 6 comprises two activities: running vulnerability evaluation tools on selected infrastructure components, reviewing technology vulnerabilities and summarizing results .

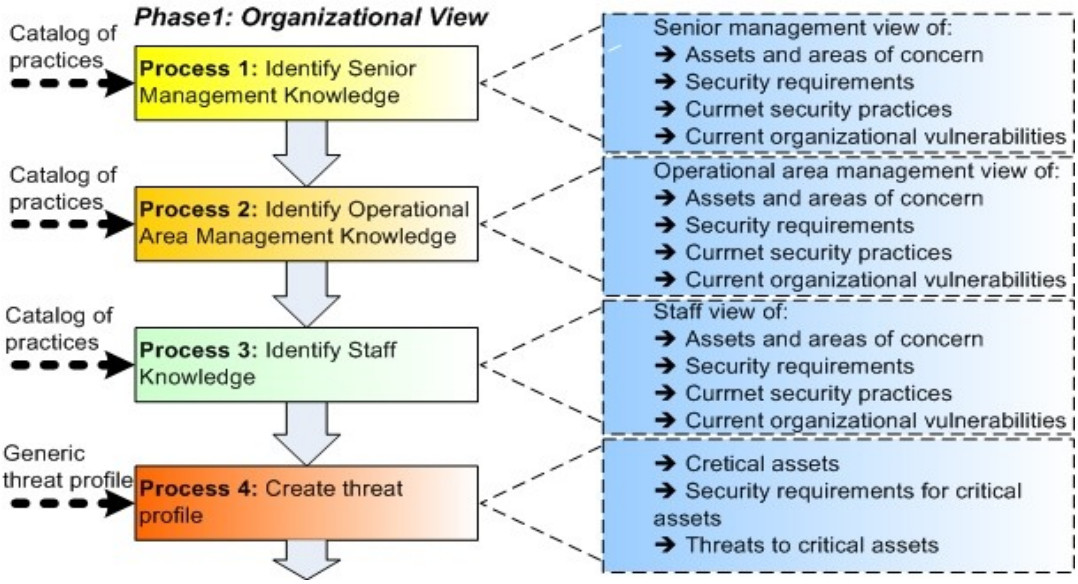

Fig. 6. Phase 1: Build Asset-Based Threat Profiles

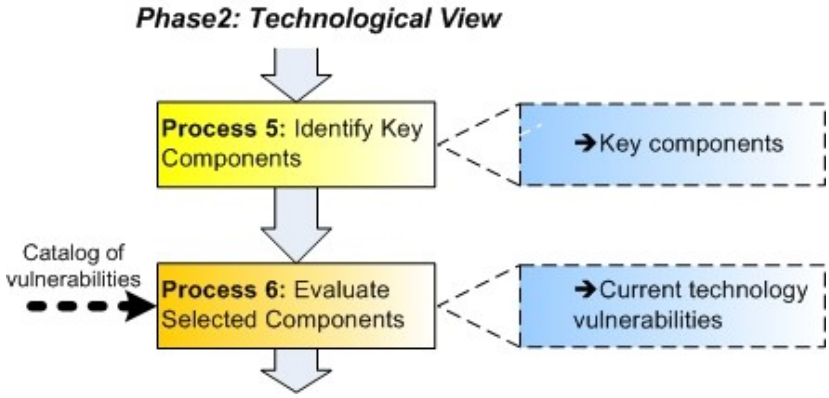

Fig. 7. Phase 2: Identify Technological Vulnerabilities.

3.4 Phase 3: Develop Security Strategy and Plans

Phase 3 is designed to make sense of the information that you have gathered thus far in the evaluation. It is during this phase that you develop security strategies and plans designed to address your organization's unique risks and issues. The two processes of phase 3 are shown in Figure 8.

Process 7: Conduct Risk Analysis. The participants in process 7 are the analysis team members, and the goal of the process is to identify and analyze risks to the organization's critical assets. Process 7 includes the following three activities: identifying the impact of threats to critical assets, creating risk evaluation criteria, evaluating the impact of threats to critical assets.

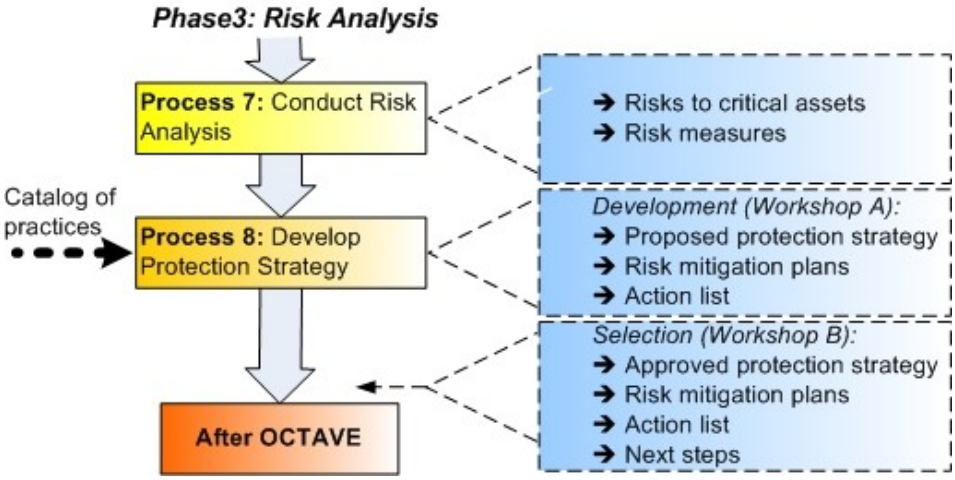

Fig. 8. Phase 3: Develop Security Strategy and Plans.

Process 8: Develop Protection Strategy. Process 8 includes two workshops. The participants in the first workshop for process 8 are the analysis team members and selected members of the organization (if the analysis team decides to supplement its skills and experience for protection strategy development). The goal of process 8 is to develop a protection strategy for the organization, mitigation plans for the risks to the critical assets, and an action list of near-term actions. The following are the activities of the first workshop of process 8: consolidation of information from processes 1 to 3, review of risk information, creation of protection strategy, mitigation plans and action list. In the second workshop of process 8, the analysis team presents the proposed protection strategy, mitigation plans, and action list to senior managers in the organization. The senior managers review and revise the strategy and plans as necessary and then decide how the organization will build on the results of the evaluation. The following are the activities of the second workshop of process 8: preparation for a meeting with senior management, presentation of risk information, review and refinement of protection strategy, mitigation plans, and action list, creation of next steps. At this point, the organization has completed the OCTAVE Method.

4 Example of OCTAVE Implementation

This case analysis is a result of conducting the OCTAVE process in a commercial healthcare institution in Poland, which is a medium sized organization. One of the main business assumptions of the described company was to protect the personal data of the patients. Taking this into consideration, we had to take account for following legal acts that are binding in Poland: Ustawa o ochronie danych osobowych - Personal Data Protection Act (29th August 1997) and Ustawa o ochronie informacji niejawnych - Confidential Information Protection Act (22nd January 1999), Norms: PN ISO/IEC 17799:2003 (BS-7799-1), PN-I-07799-2:2005 (BS-7799-2) and Tajemnica Służbowa - Confidential Information. The company also was interested in securing the computers operated by doctors and other non-medical staff. Doctors had access to confidential patient data – in Poland such data is protected by law. The company had doubts about the legal status of their existing computing infrastructure.

4.1 Systems and Databases

The main point of focus was to check if the computers in emergency rooms are properly protected and what is their threat profile. Those systems must be constantly available for use, so they are much more exposed to poten-

tial threats than an average PC. From the business point of view, any interruptions or errors would seriously threaten the quality of provided services and possibly endanger the patients. The surveyed systems reached the Impact Value of High in case of Loss/destruction. Interruption of operation unacceptable, however, it might occur. Such extraordinary events stay within the boundaries of tolerance for this organization. The results of our research were compared with the company's policy and gained acceptance.

The database that stores information about patients may be subject to unauthorized access and illegal personal information gathering. Such a crime results from improper protection of computers that have access to the database, the server on which the database is stored and finally, the database itself. This threat was marked as Medium, since it does not expose the company to direct financial losses. Modifications of the database resulting from employee negligence are important, however, their overall impact on the business process is Low, because the can be easily rolled back. The company's database backup was found to be outdated. In case of a failure, an up-to-date backup would make the effort of restoring lost information twice as fast.

4.2 Personal Computers

Internet access is a key issue in planning security structure. All personal computers (operated by medical and non-medical staff) have internet access. In our assumptions we determined that they are not a vital tool of work, but seriously improve the business process, when present. In our research we took account of such factors as: disclosure, modification, loss or destruction and unavailability of information on personal computers. Since the organization operates on 24/7 basis, also its personal computer should be able to operate constantly and the staff should have permanent access to them. This can be achieved by employing the basic rules of security, such as using sufficiently strong passwords. Loss/destruction of PCs has a critical meaning for the organization, since it could lead to an interruption of the business process together with financial losses. The same applies to Interruption and Modification, particularly in relation to applications that support the operation of medical systems.

4.3 Documentation

The documentation section includes both the documents related with the operation of the t company itself and documents related with the patients, for example, patients medical histories. Documentation should be available in electronic and paper form. There should be permanent access to the documents and they are to be stored in a logical structure. We were able to observe a tendency to store documents on desks. This should never happen; important documents are not to be placed in easy to spot locations. Only staff that runs the documentation or requires it for their work should have access to the documents. Any change in patients' files may directly affect their health, which is unacceptable. Our research also included the possibility of complete destruction of the documents (fire, water etc.). In phase one, according to the OCTAVE methodology, we determined the main assets of the company, as well as their access paths. We analyzed in detail the access to documentation, PCs, databases (of patients and staff) and systems running dedicated applications enhancing the business development. The biggest problems were the PCs – they were poorly or not at all protected. Also documentation storage proved to be a troublesome area as well; we suggested a separate room, or a place in a room, which only a limited number of employees could access. As far as network structure is concerned, we suggested the purchase of a quality software firewall, which should eliminate the risk of viruses or any sort of malware penetrating the network (at least to the Medium level). Further research revealed that computers often lacked updates of operation systems. The company should also consider training its staff in the field of security; such a training should include basic issues of computer operation with stress on security and making the staff aware of the dangers resulting from internet access. The remaining resources shall not be discussed in this article.

4.4 Survey

Additional surveys were conducted in the following groups of employees: Senior Managers, Operational Area Managers, Staff, IT Staff. The majority of departments produced similar answers. The most disturbing answers concerned the lack of a business continuity plan and the fact, that the staff did not understand its role in resource protection. This leads to a situation where people fail to comply with many regulations, because they are not aware of the danger. The IT staff was proven to be poorly trained and was unable to properly train the remaining staff. The lack of proper internet advertising was also noted. The employees claimed that they require better hardware and that it takes time to purchase some, which brings us to the conclusion that the company's budget is not particularly big in this field. The company did not conduct any sort of security audits. All employees claimed that the company did not possess the full documentation required by organizations controlling the legal status of the company. The majority did not know to who they should turn in case of a critical situation. The above conclusions close the phases 2 & 3.

4.5 Summary of Presented Example

The Network Infrastructure Map is shown in Figure 9. Emergency rooms are not included. Exclamation mark highlights the critical assets of the company. Personal computers (especially containing data of Medical Stuff) are themselves the system of interest.

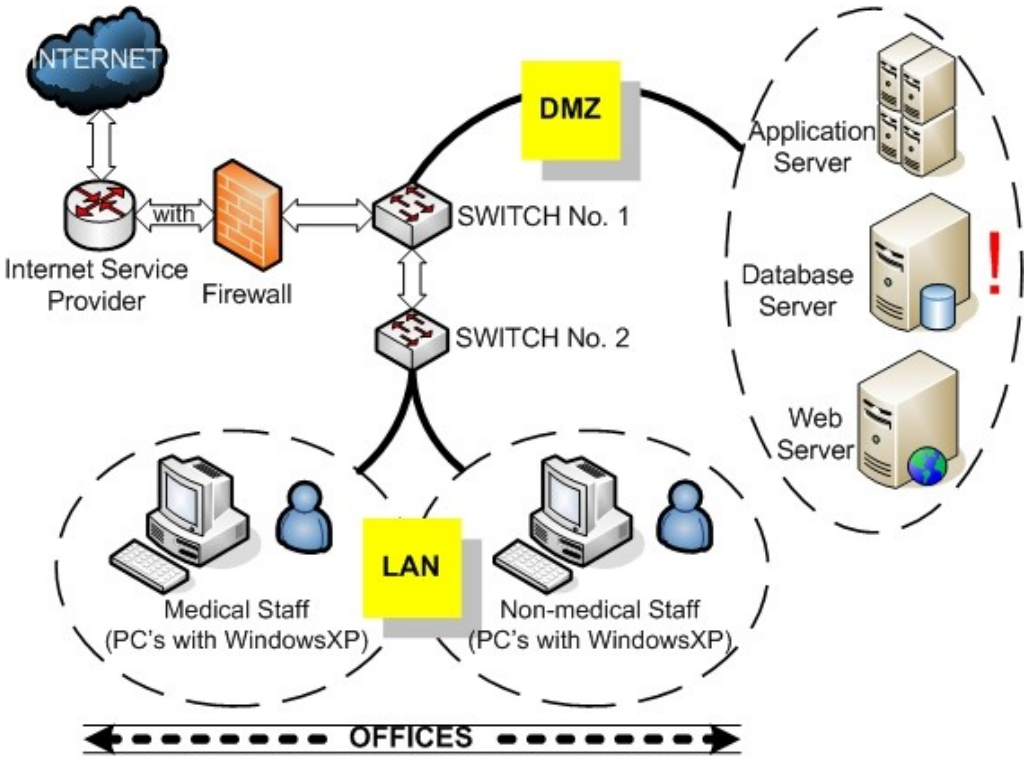

Fig. 9. Network Infrastructure Map.

The conclusions we drew during the implementation of OCTAVE methodology were based on a 3 level grade: High, Medium, Low [5]. These expressions described the level of influence of a particular phenomenon on the everyday functioning of the company. We also considered the influence of the patients and the employees' attitude towards the strategy that the company was using before our surveys. Our Evaluation Criteria

included following areas: health of customers, customer confidence and reputation, productivity, legal penalties, finances and other.

We assume that the criteria developed by us, should become a standard for the surveyed company. The above summary is a complete set of processes that make the OCTAVE methodology. After receiving the report from the workshops, the company should undertake proper steps in order to eliminate all High-severity vulnerabilities, the remaining ones should be eliminated in the course of a month.

5 Summary

Currently a few threat management methodologies exist, including ENSI TISM, Microsoft MSF, MOF and, of course, OCTAVE, which is described in this article. Each of the mentioned methodologies puts stress on different elements or forms of resource analysis teamwork organization, but all of them have the same purpose: to improve the security level of our systems and data. The choice of a proper methodology depends on the company-specific factors, but the authors are trying to point out that using OCTAVE allows for developing security principles, which are well adapted to the Polish market and company profile. The company workshops, which are described above in detail, are a huge innovation in work organization. Thanks to such approach, all participants feel to be the authors of the policy implementation and bear the moral responsibility for it to some extent. The described example of OCTAVE implementation proves that this methodology is as efficient as other methodologies used commercially these days. The attractive approach to teamwork in this methodology allows the authors to forecast an increase in the amount of its implementations.

References

1. Ustawa o ochronie informacji niejawnych z 22 stycznia 1999 r. z późn. zm. (Dz. U. 1999 Nr 11, poz. 95).
2. Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. 1997 Nr 101, poz. 926).
3. Tajemnica Służbowa, Tajemnica Bankowa.
4. Norms: PN ISO/IEC 17799:2003, PN-I-07799-2:2005.
5. OCTAVE Method Implementation Guide Version 2.0.
6. OCTAVE-S Implementation Guide, Version 1.0.
7. TISM (TOTAL INFORMATION SECURITY MANAGEMENT) – documentation, version 1.4 RC 1.
8. Andrzej Białas: *Podstawy bezpieczeństwa systemów teleinformatycznych,* pod red. Andrzej Białas, Gliwice: Wydawnictwo Pracowni Komputerowej Jacka Skalmierskiego (2002).
9. Krzysztof Liderman: *Podręcznik administratora bezpieczeństwa teleinformatycznego,* MIKOM Warszawa (2003).
10. CERT *Polska- Annual Report 2005* and `http://www.cert.org/octave/`
11. Symantec Internet Threat Report (September 2005).
12. J. Stokłosa, T. Bilski, T. Pankowski: *Bezpieczeństwo danych w systemach teleinformatycznych,* Wydawnictwo Naukowe PWN Warszawa (Poznań 2001).
13. Rafał Łukawiecki: *A Holistic View of Enterprise Security,* Project Botticelli Ltd.