Information Security Risk Assessment in Financial Institutions Using VECTOR Matrix and OCTAVE Methods

Davor Maček,
Zagrebačka Banka d.d.
Paromlinska 2, 10000 Zagreb, Croatia
davor.macek@gmail.com

Ivan Magdalenić, Nikola Ivković
Faculty of Organization and Informatics
University of Zagreb
Pavlinska 2, 42 000 Varaždin, Croatia
{ivan.magdalenic, nikola.ivkovic}@foi.hr

Abstract. *This paper describes and compares methods for assessing information security risk in financial institutions. For different types of information assets is necessary to apply different methods of security risk assessment. In this paper, a VECTOR method is described and recommended for security risk assessment that can be used in defining the priorities of critical risks. For conducting a more detailed level of security risk analysis it is recommended to use the OCTAVE method. Both methods are applied to a real case scenario and their strengths and weakness are compared.*

Keywords. risk assessment, information security, VECTOR, OCTAVE, financial institution, bank

1 Introduction

Information is actually the property as well as other business assets. It is essential for an organization that information is suitably protected. This is especially important in a business environment that is increasingly internetworking with each other and where the information is exposed to a growing number of different types of threats and vulnerabilities. Information can exist in various forms. It can be printed or written on paper, stored or electronically transmitted by regular mail or electronic means, shown on film or in the form of conversation. Information stored in all those formats must always be protected appropriately.

According to KPMG, one of the world's largest auditors, what hasn't been assessed, can't be managed [7]. So, the first step in protecting the information is security risk assessment of equipment and procedures used for information processing and storage. This is especially important for financial institutions where the exploitation of vulnerabilities in information security can lead to significant loss of reputation or direct financial loss.

In this paper we present and compare two methods for information security risk assessment. VECTOR Matrix is a method for self-assessment of information security risks. It is a good method for defining priorities of critical risks. OCTAVE is a more detailed method for assessing information security risks. It is specially recommended for security risk assessment of information containers. The both methods are used to assess security risks in financial institutions.

The paper is organized as follows: Related work is presented in section 2. The VECTOR Matrix method is described in section 3, which is followed by description of OCTAVE method in section 4. In section 5 is given comparison of these two methods. The conclusion is given in section 6.

2 Related work

Besides OCTAVE Allegro method, also National Institute of Standards and Technology (NIST) recommendations can be used for information security risk assessment in the financial industry. The risk assessment according to NIST proceeds in nine steps followed by assortment of the measures for mitigating risks [2], similar to the OCTAVE method.

OCTAVE method can be additionally supplemented by setting a time frame when selecting measures for information risk reduction, as defined in the NIST recommendations. Compared to the NIST recommendations, OCTAVE method is a more accurate and gives better overall picture related to observed information risk.

According to NIST recommendations, the first step in risk assessment for an IT system is to define

the scope of the effort. On the other hand, the OCTAVE Allegro method first developed criteria for measuring risk in accordance with organizational guidelines, because the criteria for measuring risk form the basis for risk assessment of information assets of an organization. Without such criteria, it would not be possible to measure the extent to which the organization is exposed to an impact if the risk is realized for information assets. The most important criteria for measuring risk in financial institutions are Reputation and Customer Confidence, Financial, Safety, and Legal Fines and Penalties. Those criteria must also be prioritized, and for financial institutions Reputation risk was the highest priority which can imply unwanted customer loss.

A deficiency of NIST recommendations is that the first step defines the boundaries which will be observed, but without clear criteria for measuring the risk that should be the basis for defining the scope. For this reason, for financial institutions it is still acceptable to use OCTAVE Allegro method. Also, the OCTAVE Allegro method is several years newer than NIST recommendations, and considering the dynamics of change in today's complex and volatile business environment, particularly in the financial industry, OCTAVE Allegro method would therefore still better fulfill the needs of financial institutions regarding information security risk assessment.

In its publication, the OCTAVE Allegro method also provides concrete and quality examples of risk assessment and measures for mitigation risks, which is the method really acceptable for use in the financial industry than other methods and recommendations.

Financial institutions that operate in Republic of Croatia rarely use any methods or standards like OCTAVE. Although the banks are regularly audited by PCI DSS audit, often PCI DSS is not used. In order to reduce operational risk, banks mostly use the guidelines for information system management prescribed by the Croatian National Bank [3], which are based on standards ISO/IEC 27001:2006 and BS 7799-3. The Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information [4]. Nevertheless, financial institutions mostly use NIST recommendations and SANS guidelines. To some extent, there is also used Microsoft Security Compliance Manager, baseline recommendations to efficiently manage the security and compliance process for the most widely used Microsoft technologies [9].

SANS guidelines for security risk assessment in financial institutions that are taken from Federal Financial Institutions Examination Council (FFIEC) and other financial regulators from United States outline four information security assessment processes [6]:

1. identifying the risks that can threaten customer information, which includes information gathering, analysis and prioritizing
2. development of a written plan containing policies and procedures to manage and control all identified risks
3. implementation and testing of security controls
4. monitoring and updating security plan.

Information gathering, the first phase of risk assessment according to SANS guidelines starts with a step which requires a listing of assets, including equipment, human resources and services used or planned for the system. Thus, SANS guidelines would be similar to VECTOR Matrix in a certain way, because their first step identifies critical assets. The other two steps include identifying the potential threats and obtaining owner's classification of the data in regards to its sensitivity. In the fourth step, it's needed to identify organizational and technical vulnerabilities and obtain the owner's ranking on the impact to the business of a loss in each of the following security objectives: Availability, Integrity, Confidentiality, Accountability and Assurance. Those five important business goals are set clear and correctly, but unlike OCTAVE Allegro method, currently there are no risk measurement criteria in SANS recommendations. In OCTAVE Allegro method, security goals are defined in step two while developing an information asset profile which is the step after establishing risk measurement criteria, and that would be crucial.

Consequently, OCTAVE Allegro method would take precedence and fulfill better for information security risk assessment in the financial industry than SANS guidelines. Just like NIST recommendations, also SANS guidelines are several years older than OCTAVE Allegro method, which means that those recommendations and guidelines should be updated to better fulfill information security risk assessment requirements in financial institutions.

The reasons why security staff in many financial institutions is accustomed to use older recommendations like NIST and SANS, but not yet OCTAVE method would probably be that OCTAVE method is not yet well known and not enough presented worldwide. Also, because of the dynamics of change in information technology, many security specialists unfortunately have no spare time to get educated and adopted some new methods and techniques in the area of information security risk assessment.

The risk assessment methods can be divided into two main groups: the empirical methods, usually derived from a formalization of best practices, and the theoretical ones, justified by a formal model of some sort. In everyday practice, the first group is preferred since its methods provide reasonable risk evaluations.

A good risk assessment method should be both practical and theoretically sound [10]. OCTAVE Allegro method fits both conditions.

3 VECTOR Matrix method

VECTOR matrix is free, open source and quite simple qualitative self-assessment risk method, and was developed to help business systems in defining the priorities of critical risks, including information security risks. The method allows users to easily quantify and visually represent all possible aspects of risk to the business system. VECTOR method is based on universal principles of business risk, scalable for both, small businesses and large enterprise systems, in domestic and international private sectors [1].

VECTOR method for risk assessment is based on the following formula:

RISK = V+E+C+T+O+R

VECTOR is the acronym derived from the following English words:
V = Vulnerability,
E = Ease of Execution,
C = Consequence,
T = Threat,
O = Operational-Importance,
R = Resiliency.

Vulnerability is a characteristic of a property or business process to indicate its weakness to some kind of attack. Vulnerability is linked to a threat that exploits it.

Ease of Execution is parameter that describes attacker needed level of expertise, knowledge, advanced training, special tools and equipment and time to successfully carry out an attack on an information system. Low level of ease of execution means that an attacker must invest much more effort and knowledge to successfully break the existing security mechanisms. A high level of ease of execution means that an attacker needs minimal effort for the successful penetration and unauthorized entry into the information system of an organization.

Consequence represents a loss of economic, symbolic or psychological value for organization (i.e. reputational risk for the bank in case of loss or theft of data, unavailability of certain parts of information systems, reduced levels of service quality, etc.).

Threat represents the probability of an event in which an attacker will make damage to particular business system. The analysis of threats is the first step that needs to be done in the process of risk assessment. There are various sources and forms of threats. Some of the most important threats in financial institutions are unauthorized access, malicious programs like viruses and worms, interception, disclosure of the business secret communications, denial of services that must be available 24x7, such as internet banking.

Operational importance is the measure of importance of certain asset in the overall mission of the organization. Assets with higher value are critical assets. If those assets are stopped or inactive, they can stop all other operations. On the other side, assets with a lower value may have only minimal impact on the mission in case of attack. Redundant systems could reduce the operational importance. During an initial organizational assessment, it is important to analyze a comprehensive list of assets and business processes to ensure that they covered all aspects of business risk. For example, assets that can be considered a low value upon initial inspection may later prove to be the critical component or a key process in the broader context of business. In addition, it is important over time to ensure that business systems are up to date list of its assets.

Resilience or elasticity is the speed with which the organization can successfully recover, reorganize itself and prepare to resume operations after a significant violation or failover of prescribed security policies. Risk scoring for this criterion is based on the inverse relationship. The high level of resilience (e.g. rapid recovery with minimal or no outage time) result in low level of risk scoring. On the other hand, when assets are low-level resistance (eg, when there is no redundant system, there is no backup data, there is no backup location, etc.), then this is a very high score for risk.

Table 1 shows the risk assessment of information security in bank developed using VECTOR method. Risk values are as follows: 1-4 low, 5-7 moderate and 8-10 high level of risk levels for each VECTOR.

Table 1. Risk assessment of information security in bank developed using VECTOR method

Assets		Num	V	E	C	T	O	R	Sum
Work station		V_1	8	10	8	9	8	8	**51**
Servers	Mainframe	V_2	3	1	10	1	9	2	26
	AIX	V_3	4	3	9	2	8	3	29
	Windows	V_4	7	7	8	7	8	7	44
Databases	IBM DB2	V_5	4	2	9	3	8	3	29
	Oracle	V_6	5	4	8	3	7	4	31
	MS SQL Server	V_7	8	7	7	6	6	5	39
Network devices		V_8	8	6	9	7	10	7	**47**
Firewalls	Network level	V_9	6	3	7	5	7	5	33
	Operating	V_{10}	9	9	9	10	9	9	**55**

	system level								
Physical objects	System hall	V_{11}	4	3	9	2	10	5	33
	Backup center	V_{12}	4	1	5	1	2	1	14
Intellectual property	Applic ations	V_{13}	5	6	8	6	8	7	40
	Docum ents	V_{14}	6	8	8	5	7	5	39
Information staff		V_{15}	7	5	6	4	7	7	36

The first column in the matrix is used to describe the important assets, business processes or business functions that support the overall operations of the bank. For each of those assets there are analyzed VECTOR criteria to determine the risk of the observed property or business functions in relation to other assets within the business system, in this case the bank. Table 1 shows that the largest sums of vectors have a workstation (51), network equipment (47) and firewalls at the operating system (55), which means that the risk for these types of assets is the largest.

It is important to point out that criticality of certain services that support the business process or business function is determined by its owner, not by IT staff. As business owners are responsible for identifying the impact of a risk, they are also in the best position to articulate the business value of assets that are necessary to operate their functions [8].

4 OCTAVE method

OCTAVE method is developed at Software Engineering Institute, Carnegie-Mellon University [5]. OCTAVE is a set of tools, techniques and methods for risk assessment and strategic planning of information security. OCTAVE is an acronym of the following English words:

O=Operationally,
C=Critical,
T=Threat,
A=Asset,
VE=Vulnerability Evaluation.

There are three OCTAVE methods:

- original OCTAVE method, which is the foundation of all knowledge for OCTAVE;
- OCTAVE-S - designed for smaller organizations;
- OCTAVE Allegro - a streamlined approach for assessing and ensuring information security, designed for larger organizations.

OCTAVE method is based on the OCTAVE criteria, which are actually standard approach to risk assessment and information security practices. OCTAVE Criteria sets out the basic principles and attributes of risk management using OCTAVE method. Since financial institutions are generally larger organization, the OCTAVE-Allegro method is the most appropriate for them.

OCTAVE Allegro is composed of eight steps divided into four phases:

1st Phase - Participants develop evaluation criteria for measuring risk in accordance with organizational guidelines: the mission of the organization, organizational goals and critical success factors.

2nd Phase - Participants prepare profile of any critical information assets with which to establish clear boundaries for the property, identify its security requirements and identify all of its containers.

3rd Phase - Participants identify threats to each information asset in the context of container and property.

4th phase - participants identify and analyze risk information assets and begin to develop approaches for reducing risks.

The eight steps of OCATVE Allegro methods are:

1. Criteria establishment for measuring risk
2. Development of the information assets profile
3. Identification of containers of information assets
4. Identification of areas of interest (concern)
5. Identification of threats scenarios
6. Risk identification
7. Risk analysis
8. Selection approaches for risk reduction

In Tables 2-5 is described risk assessment for logs with ATM made by using OCTAVE Allegro method based on the previously given steps.

Table 2. OCTAVE Allegro - header

OCTAVE Allegro	
Information property	Logs with ATM
Area of concern	Data bank customers can be stolen and released because of unauthorized access to workstations on which there is no Windows Firewall.

Table 3. OCTAVE Allegro - Threat

Participant *Who could exploit the weakness?*	Unhappy bank employee
Method *How could an employee take advantage of weakness?*	Bank employee could deploy malicious software by using their own workstations and make an attack on other workstations that do not have a Windows Firewall.
Motivation *What is the participant's reason to do that?*	He wants to harm the reputation of the bank because of its own status and income.
Outcome *What would be the result of the impact on information assets?*	**Announcement** Modification Annihilation Interruption

Security requirements *How to violate security requirements?*	Only authorized person can retrieve, view, store and distribute the logs from ATM with those workstations that have the Windows firewall.
Probability *What is probability to be threatened by such a scenario?*	High **medium** low

Table 4. OCTAVE Allegro - Consequences

Consequences *What are the consequences for the organization or the owners of information assets as a result of violations of safety requirements?*	**(8) Severity of consequnces** *How serious are consequences for the organization or the property?*		
	Influence area	**Value**	**Result**
In the case of disclosure of client's accounts, the bank is exposed to high reputational risk, with the possible loss of client confidence in the bank itself. A big financial loss is possible if customers decide to change the bank.	**Bank reputation and client confidence**	**High**	12
	Finance	**High**	10
	Productivity	Low	3
	Security of clients	Mediu m	5
Potential litigation	**Penalties and legal consequences**	Mediu m	**8**
The relative risk score			38

Table 5. OCTAVE Allegro – risk reduction

Risk Reduction *What action will be taken based on the total score for this risk?*	*Acceptance* *Deleying* ***Reduction*** *Insurance*
For risk to be reduced, it is necessary to do the following:	
In what container should be applied a control?	*What administrative, technical and physical controls will be applied to the container?* *What residual (remaining) risk will be still accepted by the organization?*
Workstations for pulling logs with ATM	Define the restriction on the workstations to work only with authorized persons Define security policy in such a way that users who withdraw logs do not have administrator privileges Remove all standard system shared folders The remaining risk for the bank is possibility of reading the logs by the authorized persons
Firewall	Restrict traffic on the network firewall so that workstations in ATM have open ports only for limited critical services for the recovery server (server's antivirus and security patches). In this way it reduces the scope of possible attacks, but there are still open ports for critical services to the computer.

5 Methods comparison

VECTOR matrix method and OCTAVE method are both a good choice for risk assessment of information security, but in different steps of implementation.

As a first step in risk assessment is recommended VECTOR matrix method since the method allows users to easily quantify and visually represent all possible aspects of risk of the business system. When critical risk are determinate by VECTOR Matrix method, a detail analysis of each identified risk has to be done. At this step VECTOR matrix method does not provide enough flexibility to properly describe all aspects. By using VECTOR matrix method, to each information or business asset is given a score which represent risk to a potential attack. This risk score does not provide enough information to deal with the risk, but is used to compare this risk with others in order to identify critical risks.

Unlike VECTOR methods, OCTAVE Allegro method provides much more detailed and higher quality analysis and assessment of security risks of specific information assets. By using of OCTAVE method is possible to measure more accurate and consequently better to reduce the risk of information security for a particular property. However, OCTAVE Allegro method is more complex compared to the VECTOR Matrix method, and requires much more time and effort when it is applied to the same information security risk assessment of certain assets.

Overall two described methods complement each other and are a good choice for the risk assessment in financial institutions.

6 Conclusion

Risk management is a critical point in the protection of information assets, particularly in the financial industry, hence the need for using appropriate methods and standards for information security risk assessment. The ultimate goal of such methods is to help organizations to better manage IT-related risks.

The reason for selecting the VECTOR Matrix and OCTAVE Allegro methods is that these two methods complement each other quite well during the process of risk assessment of information security in a business environment. In the financial sector, VECTOR Matrix would be first used to prioritize the critical risks, which could be made that risk assessment scales for each type of information assets. After determining the property with a high level of

risk (e.g. operating system firewall), usage of risk assessment OCTAVE Allegro method is appropriate, which is much more complex and more accurate method for qualitative analysis and security risk assessment of specific information assets. It can be said that VECTOR Matrix serves as a good groundwork to OCTAVE Allegro method for information security risk assessment.

References

[1] VECTORMatrix.com - Risk Assessment Methodology, Security, Impact Articles, U.S. Ravias Corp, available at http://www.riskvector.com, Accessed: 25th October 2010.

[2] Risk Management Guide for Information Technology Systems, Author G. Stoneburner, A. Goguen, A. Feringa: **Recommendations of the National Institute of Standards and Technology**, National Institute of Standards and Technology, Special Publication 800-30, Gaithersburg, USA, July 2002, available at http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, Accessed: 15th April 2011.

[3] The guidelines for the management information system in order to reduce operational risk, Croatian National Bank, March 2006, available at http://www.hnb.hr/supervizija/h-smjernice-za-upravljanje-informacijskim-sustavom.pdf, Accessed: 17th April 2011.

[4] Financial Services Information Security information, news and tips - SearchFinancialSecurity.com, available at http://searchfinancialsecurity.techtarget.com/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard, Accessed: 17th April 2011.

[5] R. A. Caralli, J. F. Stevens, L. R. Young, W. R. Wilson: The OCTAVE Allegro Guidebook, v1.0, Software Engineering Institute, Carnegie Mellon, May 2007, available at http://www.cert.org/octave/allegro.html, Accessed: 29th October 2010.

[6] SANS Institute InfoSec Reading Room, K. Nelson: Security Assessment Guidelines for Financial Institutions, December 2002, available at http://www.sans.org/reading_room/whitepapers/auditing/security-assessment-guidelines-financial-institutions_993, Accessed: 19th April 2011.

[7] KPMG Tanácsadó Kft, IT Advisory Services, Information Security Risk Assessment, 2011, available at http://www.kpmg.com/HU/en/WhatWeDo/Advisory/RiskAndCompliance/Risk-and-Compliance-IT-Advisory-Services/Factsheets/Documents/Information-Security-Risk-Assessment_2011.pdf, Accessed: 22nd April 2011.

[8] Microsoft Solutions for Security and Compliance and Microsoft Security Center of Excellence: The Security Risk Management Guide, Microsoft Corporation, March 2006, available at http://technet.microsoft.com/en-us/library/cc163143.aspx, Accessed: 22nd April 2011.

[9] Windows Server 2003 Security Baseline, Microsoft Security Compliance Manager, TechNet, April 2010, available at http://technet.microsoft.com/en-us/library/cc163140.aspx, Accessed: 22nd April 2011.

[10] M. Benini, S. Sicari, Risk Assessment in practice: A real case study, Computer Communications 31 (2008) 3691–3699