Methodologies and Tools of Information Security Risk Management

Bulai Rodica, Beşliu Victor

Technical University of Moldova
Str. Studentilor 7, Chisinau, MD-2012, Republic of Moldova
Tel:(37322)509908; E-mail: griniuc@yahoo.com, vbesliu@yahoo.com

ABSTRACT

Information security deals with providing protection for digital information and information systems, ensuring confidentiality, integrity and availability of data. The complexity of information security does not resume to mere technicality, transferring significant liability to proper management. The ISO/IEC 27005:2011 – Information security risk management, does not specify any particular method for managing the risks associated with information security, but a general approach. It is up to the organization to devise control objectives that would reflect specific approaches to risk management and the degree of assurance required. There have been multiple attempts to shaping risk analysis and control methodologies and tools amongst which those like CRAMM (United Kingdom, Insight Consulting), RiskWatch (USA, RiskWatch), Risicare/Mehari (France, BUC S.A./Clusif) and GRIF (Russia, Digital Security). Using the appropriate risk assessment solution, an organization can devise its own security requirements. This report deals specifically with the analysis of these methods as well the systems that use it.

Keywords: Information security risk management, CRAMM, RiskWatch, Mehari, GRIF.

1. INTRODUCTION

The fast-paced environment we live in today is indeed very difficult to keep up with. That, however, does come with the price of increasing risks which makes it imperative that organization stakeholders are brought up to speed on all the "perks" of technical emancipation. The best way to deal with information security risks is by raising awareness amongst employees and luring them to take part in identifying the vulnerabilities and threats, as well as implementing solutions to control them, therefore reducing the risks to an acceptable level.

Analysis of the risk to information security is a powerful tool that comes in handy for managers in making the decision about the implementation of efficient systems in information management, in order to achieve the organization's mission.

As a part of risk management, risk analysis is the systematic implementation of methods, techniques and management practices to assess the context, identify, analyze, evaluate, treat, monitor and communicate the risks to the information security and systems through which they are processed, stored or transmitted.

2. METHODOLOGY

2.1. CRAMM

The CRAMM (CCTA Risk Analysis and Management Method) is created by Central Computer and Telecommunications Agency of the UK government. Ever since 1985 it is used as a national standard for all governmental and commercial organizations within the UK. In the years to follow CRAMM becomes popular around the whole world. The Insight Consulting Limited Company deals with the development and maintenance of their homonymous software solution, based on CRAMM.

At present, CRAMM poses as an elaborate, universal and powerful tool which besides providing risk analysis performs auditing tasks such as:

- information system analysis and documentation estimation in accordance to all stages of analysis;
- auditing within the country's legislation and ISO 27001 – Information security management system;
- elaborating a security policy and ensuring a business continuity plan [www.cramm.com].

CRAMM uses a combination of both qualitative and quantitative analysis. It is universal and can be implemented in businesses ranging from big to small, as well as governmental or commercial. The CRAMM based software solutions used for specific types of organization can be differentiated via their profiles (Commercial Profile, Government profile). The latter supports auditing according to the American standard ITSEC (<Orange Book>).

CRAMM comprises three stages:

1 Analysis, identification and value of assets;
2 Risk identification and assessment;
3 Identification and selection of countermeasures;

Each stage requires specific data input, event sequence, interview questionnaires, check lists and guidelines.

The establishment of objectives (stage I) can be represented on a scale from 1 to 10, and it can comprise several evaluation criteria such as financial losses, loss of credibility/diminished reputation etc. Here is an example of an assessment based on financial losses and return on investment:

2 points – less than 1.000 $;
6 points – between 1.000 $ and 10.000 $;
8 points – between 10.000 $ and 100.000 $;
10 points – greater than 100.000 $.

Stage II comprises risk assessment towards the envisioned system and the security requirements. It can be represented according to the following scale: very high, high, medium, low, very low. The vulnerability level can be: high, medium or low. Taking into account these metrics, risk assessment is calculated on a scale from 1 to 7.

Stage III identifies and generates countermeasures, taking into account stage II output. The Program can suggest the following types of recommendations:

- general recommendations;
- specific recommendations;
- specific examples of security organization patterns (from the more than 1000 examples available within the database).

The main disadvantages of CRAMM:

- CRAMM requires the auditor to have special training and high qualifications;
- CRAMM is better suited for auditing an established information system as opposed to one that is still in course of development;
- CRAMM auditing can be time-consuming lasting up to several months of continuous work;
- CRAMM software solutions generate a large amount of documentation (but not necessarily useful in practice);
- CRAMM does not support pattern alteration or creation of new examples of such;
- does not support CRAMM knowledge base updating, making customization quite impossible;
- the license fee varies from 2000 up to 5000 USD.

2.2. RiskWatch

The RiskWatch software solution [www.riskwatch.com] is a powerful tool used for risk assessment. The RiskWatch software products relate to several security auditing types:

- RiskWatch for Physical Security
- RiskWatch for Information Systems – for information related risks;
- HIPAA-WATCH for Healthcare Industry – used to evaluate the compliance with the HIPAA standard (US Healthcare Insurance Portability and Accountability Act);
- RiskWatch RW17799 for ISO 17799

The RiskWatch method uses annual loss expectancy (ALE) and return on investment (ROI) as risk assessment criteria.

Unlike CRAMM, RiskWatch is mostly oriented towards a precise quantitative estimate of the ratio between security threats related loss and the cost of implementing a security system. This method takes into account information risks and well as physical risks associated to computer networks.

The RiskWatch method comprises 4 stages:

Stage I – defines the research domain. It deals with details such as the organization type, the structure of the analyzed system and basic security requirements. Based on the type of the organization there are several models/patterns (business information system, governmental/military etc) the system supports and provides then with appropriate lists of basic parameters such as protected resources, losses, threats, vulnerabilities and countermeasures. The list provides selecting aspects referring specifically to the targeted organization.

For example the losses category comprises the following:

- denial of service, delay of service;
- information disclosure;
- direct losses (i.e. equipment destruction in a fire);
- life and health (personnel, customers, etc.);
- data alteration;

- indirect losses (i.e. restoration costs);
- reputation.

Stage II – defines the input data that describes specific characteristics of the system. It can be manually fed as well as imported from reports (generated by computer networks' vulnerability assessment tools). This stage generates detailed descriptions of resources, losses and incidentals.

The potential vulnerabilities are detected through the usage of a questionnaire, containing more than 600 questions, which relate to resource categories.

The frequency of every identified threat, its vulnerability level and the resource value can be adjusted. All of the above mentioned factors are important to estimating the ultimate effect of implementing the security mechanism.

Stage III – being the most significant, deals with quantitative assessment. The risk profile is estimated and security measures are generated. The risk profile is regarded as a multitude of established links between the resources, losses, threats and vulnerabilities.

For example, a server cost is estimated to 150.000 $, while the probability of it being destroyed in a fire during a period of 12 months is equal 0,01, estimated losses resumes to 1.500 $.

The known formula: **m = p * V**, where m- waiting period, p- threat probability, V–resource value), has undergone several changes due to the fact that RiskWatch uses assessments defined by the American National Institute of Standards and Technology NIST, such as LAFE and SAFE.

LAFE (Local Annual Frequency Estimate) – i.e. a specific city.

SAFE (Standard Annual Frequency Estimate) – of a threat in a specific part of the planet, i.e. North America.

Also, a correction factor is taken into account, as the result of a threat to a resource can lead only to a partial damage to the resource and not to a complete loss of it.

The RiskWatch database covers LAFE and SAFE estimations, as well as a general description of diverse solutions. Quantitative countermeasures implementation depends of the Return on Investment coefficient for a given period of time. It can be calculated using the following formula:

$$ROI = \sum_i NVP(Benefits_i) - \sum_i NVP(Costs_i)$$

where $Costs_i$ – the implementation and maintenance cost of the security measure i; $Benefits_i$ – benefit assessment (i.e., losses cut-down), provided by security measure i; NPV - Net Present Value – inflation correction method.

Stage IV - report generation. The types of reports:
- Brief summary.
- Complete reports including all parameters discussed at Stage I and Stage II.

- Report on resource value and estimated loss from threat eventuating.
- Threats and countermeasures report.
- ROI detailed report.
- Security auditing report.

This software solution offers the possibility of assessing present risks as well as the benefits from a potentially implemented security mechanism (physical, technical, logical or other). The generated reports and graphical charts supply customers with plenty of data to assist in making/supporting their decision.

For the local market it is quite unfortunate and inconvenient that RiskWatch uses LAFE and SAFE estimations, however the method concept can be successfully adjusted, considering several factors:

- the HR factor, suggesting the availability of sufficiently trained experts that could properly estimate losses derived from security information threats;
- the availability of specific statistic information concerning information security incidents;
- the precision of a qualitative assessment regarding threat effects.

The RiskWatch solution presents the following disadvantages:

- This method does not take into account organizational nor administrative factors;
- This method does not support an integrated approach of security information;
- The RiskWatch software solution supports an English version only;
- High license fee (starting from $ 10 000 for a small sized business).

2.3. GRIF

GRIF is a complex product that provides information security risk analysis and administration. GRIF is created in 2006 by Digital Security. It produces a report on the information security resources within a system and designs an optimal solution for any type of company [http://www.dsec.ru].

The GRIF system:

- analyses and estimates the protection level of a company's valuable resources;
- estimates the potential losses of a company in terms of information security threats;
- provides an efficient risk management plan assessment along with effective countermeasures at a reasonable cost/performance coefficient;

GRIF is made up of: the information flow module and threats and vulnerabilities module.

The first comprises data on all valuable information resources and details about the users (access rights) that have access to them. It gathers info in regard to protection and security measures for each resource, the links between each resource within the network and security policies enforced by the company. The output of this system represents a complete and detailed profile of the information system in cause.

1. The user specifies all the objects that belong to the information system, such as: departments, resources, network groups, networking hardware, data types, group/user accounts and business processes.
2. The user specifies the links between the above mentioned entities. Also, the user indicates the available security/protection level of a specific resource and the information it presents.
3. The user specifies the security policies within the company, which allows an accurate estimate of the state of the current security system as well as risk assessment.

The threats and vulnerabilities module works towards identifying the vulnerabilities for every crucial resource and the possible threats that can affect with a harmful intent these weak spots. The output defines a complete report of all the weaknesses and potential attack vectors within the system.

1. The user specifies all the objects that belong to the information system, such as: departments, resources, while the objective is to reveal the systems vulnerabilities and attack vectors.

The GRIF solution comprises threats and vulnerabilities catalogues (~100 and 200 entries respectively), that assist the user in determining the threats and vulnerabilities specific to the investigated information system.

2. The user specifies the link, i.e. specific threats and vulnerabilities that concern specific department resources.

The GRIF algorithm analyses the input data and generates a report that uncovers specific risk values for every resource. A customized report can be configured depending on its purpose.
The risk management module supports risk factor analysis, provided by the user input. Consequently, defining a risk cause implies the possibility of a further countermeasure adjustment, eventually reducing risks to acceptable levels. The algorithm provides the user with an accurate description of every countermeasure efficiency prognosis as well as determines the ultimate residual risk value, leaving it up to the user to select the optimal offered solution.

Disadvantages of GRIF:

- The software is made up of too modules: the first represents a profile of the information system in cause and the last defines a report of all the weaknesses and potential attack vectors within the system.
- The software interface is not ergonomic for defining the links between system's components and there's not connection with the business process.
- The software lacks the possibility of comparing the reports at different stages of implementation of the complex of measures regarding protection.
- The lack of the possibility to complete the requirements, specific to the organization, regarding the security policy.
- The GRIF software solution supports the Russian language version only.

RISICARE/MEHARI

RISICARE considers the combination of stakes analysis, asset classification, vulnerability analysis and risk situations study to identify risks in accordance with MEHARI (Harmonized Risk Analysis Method) method [www.clusiv.asso.fr]. Risicare offers a rich interface, in the same time complex for the users and allows modeling, viewing and optimizing the obtained results.

The risk analysis used by RISICARE is based on a comprehensive threat situation knowledge base and automated procedures for the evaluation of risk reduction factors that provides a comprehensive list of risk scenarios associated with the assets and the various threats. When risk evaluation of RISICARE alleviates the user from having to make calculations and provides a measure of the seriousness of the risk of the scale in 4 levels (with a combination of the potentiality and impact) [www.risicare.fr].

Risk assessment analyses multiple threat situations (with a set of scenarios) to determine the seriousness of each risk for each attribute (such as A, l or C) of the assets and to pin-point the most serious for the organization. The Risk treatment provides simulations and optimization to select those security measures which mitigate each vital or unacceptable risk.

The process of analysis and risk assessment is done in two steps:

1. Identification of the risk. There are two ways proposed for this purpose – direct (comprising the identification of the lacks or events that might affect the information security) and system (a database is used for the automated evaluation).
2. Impact evaluation. The qualitative coefficient Ccl is used with the estimates: 1 – low exposure (disregarding any security measures, the probability of this scenario happening is very low), 2 – low impact (the probability of the scenario realization in a short or medium period of time is low), 3 – medium impact (if no actions are taken, this scenario will happen, sooner or later), 4 – high impact (if no actions are taken, this scenario will happen soon).
3. Constraint evaluation – it is performed the audit of the constraining and prophylactic factors, which might prevent risk occurring.
4. Evaluation of the protection factors – palliative (which remediate or remove) and recovery.
5. Evaluation of the probability. The possible risks are evaluated (which might happen) on a scale of 5 points: 0 – lack; 1 – very low probability of happening; 2 – low probability of happening; 3 – medium probability of happening; 4 – high probability of happening.
6. Impact evaluation, not considering the informational security countermeasures taken.
7. Impact evaluation after adopting the countermeasures of minimization and reduction of the risk indices.
8. Identification of the global risks for the organization.
9. Taking the decisions to accept the risk or not.

RISICARE displays prioritized asset protections required and security controls from the audit results, additional charts provide compliance measurement for the organization (e.g. according to ISO 27002). From these results, RISICARE allows to select additional security measures, organizational and/or technical and to integrate them into short and long term plans.

RISICARE displays currently less serious risks that may be revised in the future and they become as Accepted Risks. RISICARE may also display the risk reduction phases based on the planned improvements and the target dates for their achievements.

For each phase, RISICARE generates a detailed report with many grid results with customizable Charts and short/long term security plans.

RISICARE is delivered with a database issued from MEHARI 2010 standard knowledge base compliant to ISO 27005 requirements, description of modular components and processes. It is possible to customize RISICARE data base for specific requirements (e.g. protection of personal data) by information security experts with an additional tool: RISIBASE.
The main disadvantages of RISICARE:

- It’s a difficult tool, which requires a rich experience for configuration.
- Can be used only by the experts in the field, that are documented and know well the Mehari methodology.

3. RESULTS

Table 1. Comparison analysis of information security risk management tools

Software Solution **Comparison Criteria**	**CRAMM,** Insight Consulting	**RiskWatch,** RiskWatch	**Grif,** Digital Security	**Risicare,** BUC S.A.
Pays	United Kingdom	United States	Russia	France
Languages	English, Dutch, Czech	English	Russian	French, English
Creating	1985	- (2002, version 9)	2006	1998/1995
Licence price	CRAMM expert : £2950 per copy £875 annual license CRAMM express: £1500 per copy £250 annual license	License fee starting from $ 10.000 - 15000 per workstation Educational discount: 25%	License fee from $ 1.000 per workstation	Contact BUC SA Maintenance price: yearly fee, 15% of license price
Host operating system	Windows XP Windows 2000 Window 98	Windows XP Windows 2000	Windows XP Windows 2000	Windows XP Windows 2000 Windows Vista
Can be used	Government Agencies Large scale companies SME	Government Agencies Large scale companies SME	Government Agencies Large scale companies SME	Government Agencies Large scale companies SME
User Interface	Requires special training of the auditor	Requires special training of the auditor	User Interface is designed for IT managers and executives Does not require specific skills or in-depth information security knowledge	Requires special training of the auditor
Compliance to IT Standards	BS 7799 (ISO 27001),Cramm	ISO 17799,US-NIST 800-26	ISO 17799	ISO 27001 (mostly Plan phase), ISO 27002, ISO 27005
Functionality	**Input/Output**	**Input/Output**	**Input/Output**	**Input/Output**
Event	+/+	+/-	+/-	+/-
Action	+/+	+/-	+/-	+/-
Measure of Risk*	+/+ (Qt, Ql)	+/+(Qt)	+/+((Qt, Ql)	+/+ (Qt, Ql)
Setting the scene	+/-	+/-	-/-	+/-
Probability	-/+	-/+	-/+	-/-
Danger	-/-	-/-	-/+	-/+
Choice situation	-/-	-/-	-/-	-/-
Frequency	+/+	+/-	-/-	-/-
Expenses and losses (Costs)	+/+	-/+	-/+	-/-

*Quantitative –Qt and Qualitative - Ql evaluation

4. CONCLUSION

The theoretical model of the analyzed methodologies is hard to be put in practice, without an experience required from the members of the risk analysis team and lack of an automated tool which allows the recalibration of the method by periodically refreshing the entering parameters (goods, threats, vulnerabilities). Also, keeping track of the actions taken during the risk prevention period and, implicitly the possibility of evaluating the impact of the adopted decisions in the risk analysis period on the organization mission accomplishment is important.

This analysis reveals the fact that methodologies differ in matter of peculiarity of the steps taken and in the way the activities of establishing the security requirements are treated. Moreover, a series of lacks of the analyzed tools is presented.

In this context we propose:

- Refining some methods and making some modern tools of informational risk management accessible at the national level;
- Development of the databases which would store the series of risks, threats and vulnerabilities, as well as specific measures to prevent or diminish those, depending on the risk tolerance of each organization.
- Elaborating an additional electronic guide to make the application and usage of the tool and the security measures more explicit, which would have an educational role as well, for building and consolidating an informational security policy inside the organizations, in the context of statistics that pin-point the fact that, though essential, this element is often ignored by the managers.
- Defining explicitly the binding of the conceptual space to the practical implementation of the methods of analysis and management of the informational risks and the benefits on the way of management decision making at the organization level of any kind.
- Deciding on the information security risks management should be strongly based on proper arguments offered, adequate from the point of view of information security and efficient from the point of view of the costs.

REFERENCES

1. www.cramm.com
2. www.riskwatch.com
3. http://www.dsec.ru/products/grif/
4. http://www.risicare.fr
5. www.clusiv.asso.fr
6. http://www.27000.org/iso-27005.htm
7. http://rm-inv.enisa.europa.eu/methods_tools