UDC 624.023

Miran Vršec, Robert Brumnik, Milan Vršec

Faculty of Criminal Justice and Security, university of Maribor, Ljubljana, Slovenia

APPROACH'S TO ESTIMATE VULNERABILITY AND THREATS OF INFORMATION CRITICAL INFRASTRUCTURE

Purpose

Today's highest level of information systems security represent a cryptography and some other models of information security infrastructure. One of the main goals of the renovation of identification systems is the automation of these on the basis of our own characteristics, which enables faster, safer and more accurate information security. The purpose of the contribution is to present a model of providing information security in information critical infrastructure.

Design/Methodology/Approach

The contribution gives an overview of existing models of information security management and the new methodology approach, which is specific to the critical information infrastructure. In technology which has also expanded the ability to use, its intended use, it is extremely likely to become subject to malicious use.

Findings

This paper describes how with the proper approach to the management of information security (CRAMM (CRAMM (CCTA's Risk Analysis and Management Method) was created in 1987 by the Central Computing and Telecommunications Agency (CCTA) of the United Kingdom government. CRAMM is currently on its fifth version, CRAMM Version 5.0. It comprises three stages, each supported by objective questionnaires and guidelines. The first two stages identify and analyze the risks to the system.), ISMS (ISMS (Information Security Management System) is, as the name suggests, a set of policies concerned with information security management. The idiom arises primarily out of ISO/IEC 27001.), ISM Cube (ISM Cube (ISM3) is a a framework for Information Security Management Systems. ISM3 looks at defining levels of security that are appropriate to the business mission and render a high return on investment. URL: http://www.ism3.com/ (09.04.2009)) etc.) ensure optimal security of information systems. Consistency with the requirements established by the protection of informations and datas to the law with evaluation of security systems and with experimental methodologies.

Research limitations/Implications

Some of guidelines are purposed to help the establishment of information security management, and a few problems that may hinder the ISMS establishment and operation of such a system.

Practical Implications

In order to avoid the modern manifestations of crime (computer crime, botnet [3], DDoS, information theft, etc.) there is urgent to ensure maximum possible security based on the evaluation of information security systems with the experimental methodologies.

Originality Value

The development creates new products and services in the field of information systems. All this is consequently associated with new approach to manage risks in information security systems based on ISMS methodology mixed Boehm's model.

Paper type: *Research Paper*

Keywords: *Information Critical Infrastructure, ISMS, ISM^3, CRAMM, Boehm's model.*

1. Approach's to Information Security Risk Management

One of the most important aspects of security organization is to establish a framework to identify security- significant points where policies and procedures are declared. The (information) security infrastructure comprises entities, processes, and technology. All are participants in handling information, which is the item that needs to be protected.

Security incidents of Information Technology in practice are unavoidable. There are many ways of risk the security and confidentiality of data such as the partial destruction or loss of data, loss of credibility of information, misuse of information or capabilities of systems, or unavailability of, or impediment to the availability of data and even systems [6]. Identification of the security incident and the effective and timely response to it are crucial to reduce the effects, as soon as possible eliminate the disturbance and restore the normal situation and the possible collection relavantnih evidence of possible criminal liability of the agent [4].

The successful manage of incidents, it is necessary to prepare security system in advance that in the event of an incident in time and effectively respond, preferably already at pre-established scenario and developed tools that will enable the rapid collection of data and evidence. One approach is to set up a special response group to take the lead in coordinating activities for the duration of the incident. A successful response to the event to ensure that these and similar events in the future would not recur and to learn some lessons from that would be our response in the future more effectively [5].

Table 1 contains the RA (RA (Risk Assesment) Risk Assessment Policy document guides the activities that need to be implemented by each Business Department, Technology Department, and Corporate Department within the organization. url: http://www.supremusgroup.com/compliance_template/Risk_assessment_package.htm (09.04.2009))/RM (RM (Risk Management) for our case ITS-RM (Information Technology Risk Management) url: http://www.itc.virginia.edu/security/riskmanagement/ (09.04.2009))(products) comparable with classi-fication of ENISA(ENISA has generated an inventory of Risk Management / Risk Assessment methods. A total 13 methods have been considered. url: http://www.enisa.europa.eu/rmra/rm_ra_methods.html (10.04.2009)) in the ISMS. Number of points (•, • •, • • •) in Table 1 varies from 0 to 3. Items shown on methodologies rate of products according to the ISMS functionallity. It also shows the size of enterprise for each methodologies are designed and what level of expertise required in the implementation of application of the methodology. Furthermore, there are some details of the methodologies to process risk management and information security.

Table 1

Methodologies of information security management

Attributes / Products	Threat identification	Threat characterisation	Exposure assessment	Risk characterisation	Risk assessment	Risk treatment	Risk acceptance	Risk communication	Languages	Price (method only)	Size of organisation	Skills needed	Licensing	Certification	Dedicated support tools
Austrian IT Security Handbook	••	•	•	••	•••	•••	•••	•••	GE	Free	All	**	N	N	Prototype (free of charge)
Cramm	•••	•••	•••	•••					EN, NL, CZ	Not free	Gov, Large	***	N	N	CRAMM expert, CRAMM express
Dutch A&K analysis	•••	•••	•••	•••					NL	Free	All	*	N	N	
Ebios	•••	•••	•••	•••	•••	•••	•••	•••	EN, FR, GE, ES	Free	All	**	Y	N	EBIOS version 2 (open source)
ISF methods	•••	•••	•••	•••	•••	•••	•••	•••	EN	For ISF members	All except SME	* to ***	N	N	Various ISF tools (for members)
ISO/IEC IS 13335-2 (ISO/IEC IS 27005)	••	••	••	••	••	•••	•••	•••	EN	Ca. €100	All	**	N	N	
ISO/IEC IS 17799	•					•			EN	Ca. €130	All	**	N	Y	Many
ISO/IEC IS 27001						•	•		EN, FR	Ca. €80	Gov, Large	**	Y	Y	Many
IT-Grundschutz	•••	•••	•••	•••	•••	•••	•••	•••	EN, GE	Free	All	**	Y	Y	Many
Marion (replaced by Mehari)	•••	•••	•••	•••					EN, FR	Not free	Large	*	N	N	
Mehari	•••	•••	•••	•••					EN, FR	€100-500	All	**	N	N	RISICARE (ca. € 10.000)
Octave	••	••	••	••	••	••	••	••	EN	Free	SME	**	N	N	
SP800-30 (NIST)	•••	•••		•••	•••	•••	•••		EN	Free	All	**	N	N	

Slovenian Institute for Standardization in y.2000 translated and adopted the British Standard BS 7799:1995 (Code of practice for Information Security Management). Given the requirements for security of personal information in public administration and the banking sector (Basel (Bassel Agreement an accord developed during a 1975 meeting in Basel, Switzerland of central bankers of the industrialized nations setting forth guidelines for the supervision of banks. Included are guidelines for minimum capital requirements. The agreement was reached by the Committee on Banking Regulations and Supervisory Practices.) II-Agreement), the derivation of the project is essential. The requirements are then more frequently occurred in the economy and the private sector. Laws that would require compliance with the recommended standard, or at least put down the requirements for the protection of information in the early stages of deployment, in Slovenia it was not. By introducing ZVOP-1 (Law on the Protection of Personal Data) which based law for protection of documents and archives, and related implementing regulations and norms, the requirements to protect information and data have become virtually universal. Apply to the vast majority of people in the private sectors and goverment. The standard BS 7799 has also developed into a family of international standards ISO/IEC 27000 which is further supported by the standard 27006, and provided a global accreditation scheme, and the mutual recognition of certificates ISMS worldwide.

ISO/IEC 27000 standard cover some parts of Information Security Management:

ISO / IEC 27001:2005 Information technology – Techniques to ensure the security - Information Security Management Systems – specification with guidance (Information technology – Security techniques – Information Security Management Systems – Requirements)

ISO / IEC 27002:2005 Information technology – Techniques for ensuring safety – Code for the management of Information Security (Information technology - Security techniques – Code of practice for Information Security Management)

ISO / IEC 27006:2007 Information Technology – techniques for ensuring safety – Requirements for certification bodies (Information technology - Security techniques – Requirements for bodies providing audit and certification of Information Security Management Systems).

1.1 CRAMM Methodology.

The methodology of analysis and risk management in projects (CCTA's Risk Analysis and Management Method – CRAMM), which also needs to prepare the English government. Today is CRAMM methodology prevalent among many of the other users also used by NATO.

Although the methodology was initially intended to conduct the project on the development of information technology, is due to its flexibility exercised in all areas of expertise. It includes both managerial as well as the implementation of tasks and has to support them made a special technique (Figure 2).

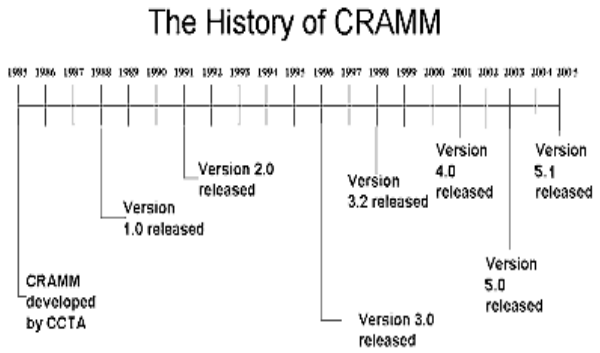

Figure 1. History CRAMM methodology and related software version

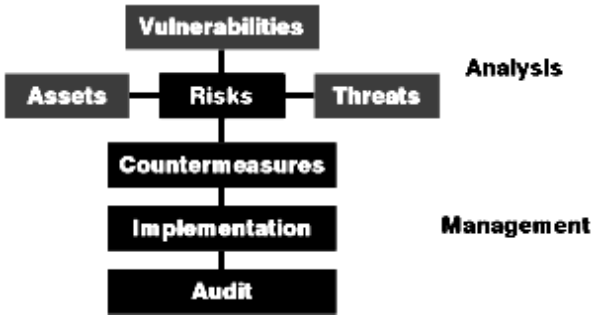

Figure 2. Analysis and risk management at CRAMM methodology

In the introduction of the methodology there are two approaches (the software package): CRAMM

Express and CRAMM Expert. History of development of the software versions shown in Figure 1.

1.2 The Information Security Management System (ISMS) Methodology.

Implementation of the management system of information security in an organization requires a good knowledge of their own assets, their value to the organization as well as their vulnerability. Take responsibility for ensuring the security of information assets means a reduction of risks to the achievement of the various threats that threaten the property. To this end, the organization set up a proper system of management. ISMS providing a framework for more effective management of security risks. For the planning and implementation suvi have recommended the following process steps:

1. Plan Phase:

– ISMS scope and approach determine to risk assessment

– Risk analysis

Identification of risks:

identification of key activities

Identification of sources of key activities

Identification of threats

– Risk Assessment

Estimate the likelihood of realization of the threat

Defining the risk profile

– Consideration of the risks

Evaluation and definition of the acceptability of risks

Identification of the risks of treatment and their analysis

– Selection of treatment measures of risk

– Obtaining the approval of the residue risk and approval of ISMS implementation

2. Pending Phase:

– Plan implementation and implement controls

– Measuring the effectiveness of controls

– Education and awareness

– Management of ISMS resources

– Management of information incidents.

3. Check Phase:

– Supervision and inspection all components of ISMS

4. Act Phase :

– Maintenance and improvements ISMS.

Model based on the PDCA methodology developed as a basis for implementing the advice in the design and implementation of information security management models in public administration and economic sector. PDCA Principle covers all phases of operation from its establishment to the mature phase of operation (Figure 3).

1.3 ISM Cube (ISM^3) Methodology.

ISM^3 (pronounced as the ISM cubed, it means the Information Security Management maturity model) is one of the newer approaches to managing information security. The model describes the maturity of information security management and is based on the standard for quality management ISO9001, with extensions for managing information security. The cornerstone of information security ISM^3 stapled defined levels of maturity in the management of the organization and allows long-term planning and adaptation to the level of security to the needs of businesses.

Figure 3. PDCA principle as the basis for the establishment of ISMS system for managing information security within an organization

ISM^3 is oriented to the process for ensuring information security and not to control. Processes are formally described, and contain the metrics and target levels of performance. It is important to have as a starting point we get a measurable information security. Organizations that manage IT services in accordance with ITIL or ISO/IEC 20000 can ISM^3 strengthen the security process.

2. Weaknesses in risk management and information security management

The problem of the standard ISO/IEC 27001 and ISMS is in the absence of step-by-step in achieving certification of compliance. From Table 1 it is clear that some of those tools are not equally supported in the stage of risk assessment and risk management of information security phases. In order to achieve maximum information security management system should be a methodology that addresses the management of security upgrade to the methodology of risk assessment, which is through the project approach in the development phase (DFMEA (DFMEA (Design Failure Mode and Effects Analysis) The DFMEA method allows the design team to document what they know and suspect about a product's failure modes prior to completing the design, and then use this information to design out or mitigate the causes of failure.), CMM (CMM (Capability Maturity Model) in software engineering is a model of the maturity of the capability of certain business

processes. A maturity model can be described as a structured collection of elements that describe certain aspects of maturity in an organization, and aids in the definition and understanding of an organization's processes.), Boehm, etc.).

3. ISMS methodology upgraded with 3D Boehm's spiral model

So it is necessary that the information security proces for critical infractructure begins with the development of applications and infrastructure. Especially in the development of information systems which we are dealing with personal information (health care, airports, police, etc.) and is constantly under development is strictly necessary to take into account all the elements for a proper construction of the software. Creation and development of the software can be placed in the Boehm's (Figure 4) spiral model of software development [2] to ensure high level of security of information system infrastrusture.

Conclusion

One of the first things recognized was that the evaluation of threats and security risks were to vague and no new security challenges were anticipated. This means being professionally and constantly in command of menacing danger, threats and business and security risks within global and European security interests also in individual sate institutions, private companies, public companies, business systems, concerns, corporations and other organizations. All this originates from natural and industrial accidents, from criminal, terrorist, spy ring and other attacks on national economies and national values. Therefore, this means a fundamental tendency towards increasing the quality of security, protection and civil defence at all levels of life, work and business operations. If we take a look at the intention of the anti-terrorist and anti-criminal coalitions we can establish that it is essentially the globalization of efforts for the security of nations, economies and populations.

Within the current of globalization, Slovenia will also be harder hit in the areas of being threatened including business and security risks.

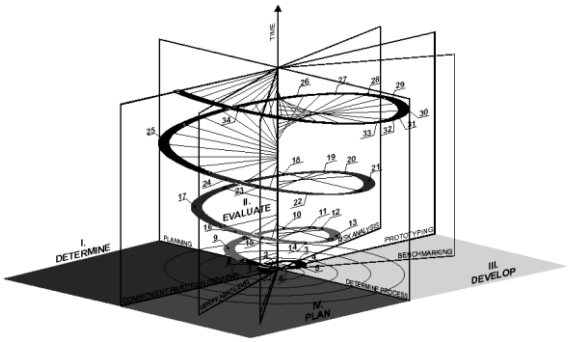

Figure 4. Boehm's model based on PDCA approach [1]

Literature and sources

1. Balantič Z. Multimedia Spiral Architecture Development for Effective Medical Education / Z. Balantič // WSEAS Transactions on Computers. – Athens & New Jersey, 2006. – 10 (5). – P. 2293-2301.

2. Boehm B. A Spiral Model of Software Development and Enhancement / B. Boehm // IEEE Computer, 1998. – Vol. 21. – 116 p.

3. Bort J. Network World / J. Bort // Attack of the Killer Bots. – 2007. – P. 29.

4. Crabb G. U.S. Postal Service Global Investigations, and Yuval Ben-Itzhak, CTO Finjan // Presentation at the Gartner IT Security Summit 2007. – Washington: DC, 2007. – 234 p.

5. Europol: Computer-related crime within the EU / Old crimes new tools; new crimes new tools. Luxembourg // Office for Official Publications of the European Communities, 2003. – 176 p.

6. Emigh A. The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond, A Joint Report of the US Department of Homeland Security / A. Emigh // SRI International Identity Theft Technology Council and the Anti-Phishing Working Group. – October, 2006. – 246 p.

Поступила в редколлегию 26.02.2009

Рецензент: канд. техн. наук, доцент С.В. Кавун, Харківський національний економічний університет, Харків.

ПІДХІД ЩОДО ОЦІНЮВАННЯ УРАЗЛИВОСТІ ТА ПОГРОЗ ДЛЯ ІНФОРМАЦІЙНОЇ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Міран Вржек, Роберт Брумник, Мілан Вржек

Сучасний високий рівень інформаційної безпеки систем у своїй основі використовує шифрування й деякі інші моделі безпеки інформаційної інфраструктури. Одна з головних цілей реконструкції систем ідентифікації - їхня автоматизація на основі розроблених власних параметрів, що забезпечує більше швидку, безпечну й точну інформаційну безпеку. Метою статті є подання моделі забезпечення інформаційної безпеки для інформаційної критичної інфраструктури.

Ключові слова: *інформаційна критична інфраструктура, ISMS, ISM, CRAMM, модель Боемса.*

ПОДХОД ДЛЯ ОЦЕНКИ УЯЗВИМОСТИ И УГРОЗ ДЛЯ ИНФОРМАЦИОННОЙ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Миран Вржек, Роберт Брумник, Милан Вржек

Современный высокий уровень информационной безопасности систем в своей основе использует шифрование и некоторые другие модели безопасности информационной инфраструктуры. Одна из главных целей реконструкции систем идентификации – их автоматизация на основе разработанных собственных параметров, которая обеспечивает более быструю, безопасную и точную информационную безопасность. Целью статьи является представление модели обеспечения информационной безопасности для информационной критической инфраструктуры.

Ключевые слова: *информационная критическая инфраструктура, ISMS, ISM, CRAMM, модель Боэмса.*