Global Information Assurance Certification Paper

A qualitative risk analysis and management tool – CRAMM
Zeki Yazar (GSEC, Version 1.3)

Abstract

Facing the emerging challenges of the Internet era, managers and information security professionals in business and government should manage specific risks to their organizations to ensure efficient operations. This paper explains basic components of risk analysis and management processes and mentions different methodologies and approaches. It then describes and discusses CRAMM, as an automated tool based on qualitative risk assessment methodology, by going through the stages of a CRAMM review, i.e. asset identification and valuation, threat and vulnerability assessment, and countermeasure recommendation. Raising organizational awareness CRAMM is a comprehensive and flexible tool especially for justifying prioritized countermeasures at a managerial level, needing, however, qualified and experienced practitioners for efficient results.

1. Introduction

Increased dependency on networked information systems, expanded internal communication facilities, explosive growth of Internet, closer ties with business partners, driven further by e-business, e-government initiatives and facilitated by the advances in information and communication technologies created many new opportunities, but also an environment with more risks than ever before.

Steve Cross of ISA, the Internet Security Alliance formed between U.S. private industry, government agencies and academic researchers in 2001, said “as the number of companies conducting business on the Internet continues to rise, so does the sophistication and number of cyber-attacks. Financial losses to business and government due to Internet vulnerabilities could exceed $100 billion per year by 2004." [DOS01]. It seems to be a realistic view, since Computer Economics, a California-based Internet research organization, estimates the economic impact of only the last four major malicious code incidents (Love Bug, SirCam, Code Red, Nimda) over $13 billion [COM02].

Based on own projections Computer Economics notes that the probability of each organization to be hit is growing: “Computer crime will grow by an estimated 230 percent during 2002. Similar trends are expected with Internet fraud, which will be up over 100 percent, and viruses, which will increase by 22 percent during the same period.” Even more disturbing is the underreporting: “According to government and industry sources, only about 20 percent of computer security violations are actually reported.” [COM02].

A recent CERT Coordination Center paper [CCC02] gives an overview of attack trends as follows:

- automation; speed of attack tools,
- increasing sophistication of attack tools,
- faster discovery of vulnerabilities,
- increasing permeability of firewalls,
- increasing asymmetric threat,
- increasing threat from infrastructure attacks.

Let me give two striking examples for the mentioned trends: Code-Red (CRv2) infected more than 359,000 computers worldwide in less than 14 hours [CAI01]. CERT/CC reports 2,437 vulnerabilities in 2001, almost six times more than 417 in 1999 [CST02], not to mention the unknown vulnerabilities.

Facing with these emerging challenges and considering other aspects like the generally more widespread insider threat and the non-technical information security leaks, managers and information security professionals should evaluate the specific risks to their organization to ensure an appropriate level of security enabling a seamless flow of their business operations.

In the present competitive environment however, most managers tend not to rely on some general statistics or projections, when it comes to invest in information security measures which may reduce IT performance or employee productivity, while not providing any tangible benefits. While these organizations may suffer serious losses due to security breaches, others may not be sure whether they over-protect their assets by supporting security initiatives, which may also result in loss of competitive advantage. The tool that should fine-tune and justify the required security measures and pave the way for informed management decisions is risk analysis and management.

2. Risk analysis and management

Risk, the possibility of damage or loss, is described mostly in dependencies of threat and vulnerability, or impact and probability. The general framework developed in 1992 NIST workshops cited in [CRA98] formalized six concepts in risk analysis: “(1) assets, (2) vulnerabilities, (3) threats, (4) impacts, (5) likelihoods, and (6) safeguards.” In another framework Ozier lists twelve elements of risk by indicating quantifications and dependencies (e.g. motivation, capability and resource availability for threat agents) for some of them [OZI99].

There is a wide consensus among information security professionals that there can be no 100% security, or in other words no zero risk. Even assuming that a

complete risk elimination is possible, this would rather be hindered by budget constraints or in most cases not attempted since measures would cost more than the asset value to be protected. Thus the emphasis of dealing with risks in this context moves from risk avoidance to risk management.

Basically risk analysis and risk management are defined as follows [CHI97]:

> Risk analysis involves the identification and assessment of the levels of risks calculated from the known values of assets and the levels of threats to, and vulnerabilities of, those assets.
>
> Risk management involves the identification, selection and adoption of countermeasures justified by the identified risks to assets and the reduction of those risks to acceptable levels.

Thus the measure of risk can be determined as a product of threat, vulnerability and asset values:

> Risk = Asset x Threat x Vulnerability

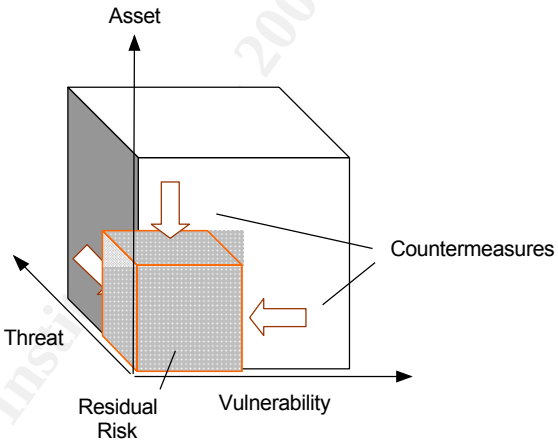

Figure 1: Risk as a function of asset value, threat and vulnerability [BRE99].

The risk elements and their corresponding countermeasures can best be visualized with a cuboid (Figure 1). The system has an initial level of risk before any countermeasures are applied. Countermeasures, assuming that their values are assigned by the same parameters that are used for threat, vulnerability and asset valuation, can reduce risk, i.e. by reducing threat (e.g. locked doors, firewalls), reducing vulnerability (e.g. awareness, patches, hotfixes) or reducing asset value (e.g. encryption). After calculating the results from each combination of threat, vulnerability, asset and countermeasure the residual risk is determined

[BRE00]. Here the impact element is covered in asset value, the likelihood in threat and vulnerability values.
Considering their business environment and resources available the decision-makers in an organization may then implement one or more of the following risk management strategies:

- risk mitigation (reducing the risks with applying selected countermeasures),
- risk acceptance (accepting the residual risk or even the initial level if the countermeasures are more costly than the asset values),
- risk transfer (transferring the risk to another organization, e.g. by insurance or outsourcing).

The option of eliminating assets may also be mentioned here in case of very high risk, unavailable or unaffordable countermeasures as well as impossible risk transfer.

There are several methodologies from the 1970's U.S. government FIPS 65 guideline (withdrawn in 1995) for performing risk analysis in large data processing centers [GIL89] to the recent approaches, which attempt to adapt to technological advances like Internet by prototyping real-time risk analysis [VEN99] and emerging applications like e-commerce by using case-based reasoning [CHA99] or consider a framework for the "whole system" during the risk management life cycle [CRA98]. In the latter work and especially in [LAB99] three generations of risk analysis and management methodologies are identified and their shortcomings discussed, in which the first generation corresponds to mainframe era, the second to networks and distributed computing, and the third to open environments and Internet.

Today most current risk analysis methodologies start with identifying and valuing assets, followed by identifying threats likely to occur to them with related vulnerabilities. Finally risk is determined for combinations of identified assets, threats and vulnerabilities to propose appropriate countermeasures. During this process two different measurement schemes can be applied to risk elements; quantitative or qualitative. Quantitative approach articulates risk in numerical terms, i.e expected monetary loss and probability (e.g. annual loss expectancy, ALE). Qualitative approach has no numeric value and is usually opinion based. Results are summarized in words like "low", "medium" and "high". Advantages and disadvantages of both approaches are listed in several works including [KRA99].

There are a wide range of threats and vulnerabilities as well as different business environments and solutions with the need for balancing organizational and technical issues. This makes the implementation of risk analysis and

measurement methodologies difficult and their outcome dependent on the experience of the persons involved, which causes inconsistence and sometimes unsatisfactory results. Moreover they require big amount of information to be gathered and a number of – by quantitative methods especially complex - calculations to be made. In order to address these problems automated tools are developed to raise the productivity by minimizing work and analysis time, as well as normalize differences of personal experience. There are a number of risk management packages listed in [NIS91], which gives an idea on different implementations, although the information is not up-to-date.

Next section will take a closer look at one of those tools, namely CRAMM.

3. CRAMM

CRAMM (CCTA Risk Analysis and Management Method) is a qualitative risk analysis and management tool developed by UK government's Central Computer and Telecommunications Agency (OGC since April 2001) in 1985 to provide government departments with a method for information systems security reviews. The tool, which has undergone major revisions (currently in Version 4), is later commercialized and now distributed by a UK firm, Insight Consulting, as "CRAMM Manager" (alongside the UK Security Service). There are around 500 copies in use in 20 countries including commercial organizations [CUG02].

The CRAMM overview below is based on referenced information available on the Internet (including [GAM97] and [SCO01]), as well as the 'CRAMM User Guide' [CUS01] and the presentations I attended.

CRAMM can be used for all kinds of organizations in,

- justifying security or contingency related investments for information systems and networks by demonstrating need for action at the managerial level, based on quantifiable results and countermeasures from organization-specific risk analysis, or
- demonstrating compliance with BS7799 (the British standard for information security management) during a certification process.

It may also be regarded as a benchmark to organizations for risk and contingency management considering the input from a number of government and private sector security experts in the tool.

The essential elements of data collection, analysis and output results, that should be present in an automated risk analysis tool [GIL89] are covered in the three stages of a CRAMM review:

- identifying and valuing assets,

- identifying threats and vulnerabilities, calculating risks,
- identifying and prioritizing countermeasures.

CRAMM tool guides the review with a process-flow oriented interface (Figure 2).

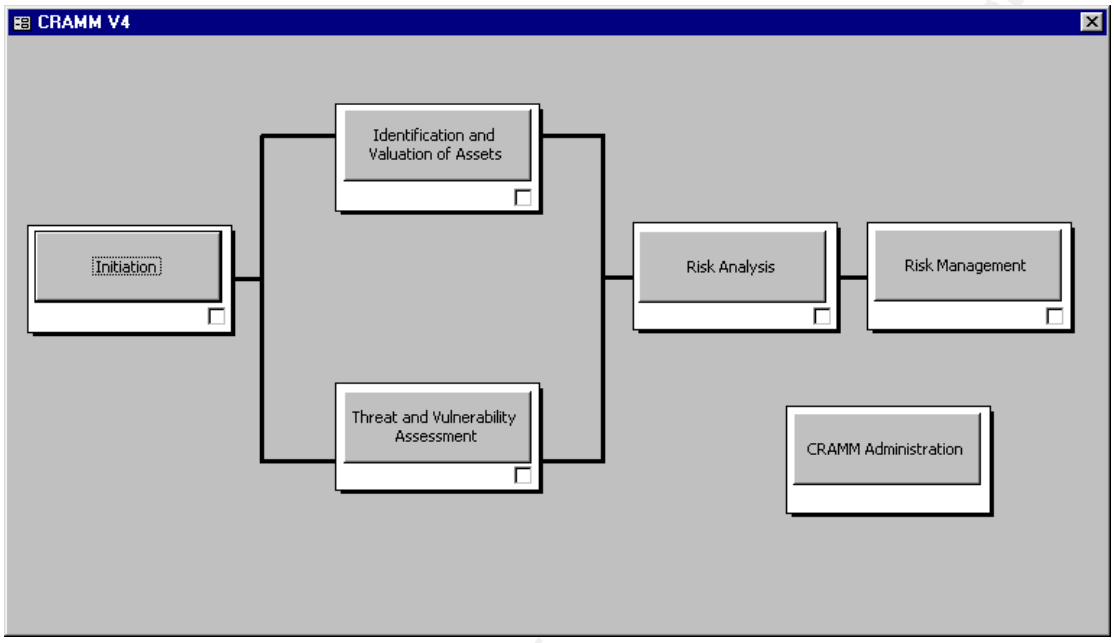

Figure 2: CRAMM overview screen [CUS01].

3.1. CRAMM risk analysis

3.1.1. Initiation

CRAMM methodology make use of meetings, interviews and structured questionnaires for data collection. In the starting phase of an analysis the initial meeting with reviewers (persons conducting CRAMM reviews, who need to be trained and experienced in using the tool) and management of the organization is important to set objectives, scope and boundary of the review, terms of reference, project structure, schedule and deliverables, as well as to identify interviewees. The results are documented in a 'Project Initiation Document'.

3.1.2. Identification and Valuation of Assets

Asset values to an organization are central in determining the risks and the required security level. Three types of assets that make up the information are identified: data, application software and physical assets (i.e. equipment, buildings, staff; assessed with locations where appropriate). With CRAMM all

interrelated assets, including end user services to differentiate the processing of data (e.g. e-mail, interactive session, Web browsing), can be defined in asset models, which can reflect business processes. Modelling is one of the most critical issues in using the tool, since too fine granularity here may unnecessarily extend the review process, while a too coarse one may miss important assets causing misleading results.

The valuation of information assets is regarded sometimes as a speculative activity, since it depends on who (e.g. sensitive information in hands of a competitor or a script-kiddie) and when (e.g. expirable passwords) possesses them. In CRAMM the reviewer conducts interviews with “data owners” (e.g. business unit managers) to value data assets, which raises the level of organizational acceptance of the review. This part of valuation is more difficult, since it may be hard to identify data (or business process) owners sometimes, or the interviewees may need some guidance for estimations, which may also be regarded as an awareness process.

Values are derived from the impacts of breaches of confidentiality, integrity, availability and non-repudiation, the widely accepted principles of information security. The interviewees describe reasonable worst case scenarios and outline the possible consequences of the data being unavailable (e.g. for several time frames between “less than 15 minutes” and “2 months and over”), destroyed (e.g. loss of data since last backup), disclosed (to insiders, contracted service providers or outsiders) or modified (e.g. keying errors, mis-routing, insertion of false messages). This approach is regarded as a shortcoming in [LAB99], since worst-case scenarios can be extremely unlikely in the real world and “can easily be used to distort a situation”.

The defined severity of impacts are then compared with an appropriate guideline (e.g. “financial loss/disruption to activities”) provided by the tool to derive an asset value within the scale of 1 to 10. The customizable range of values (e.g. “1” for “losses of $1000 or less”, “2” for “losses of between $1000 and $10,000”, etc.) defined in the guidelines avoid the difficulty of making single-point estimates. For financial loss scenarios, the actual financial loss can also be assessed.

Application software and physical assets are more easily valued by interviewing “support personnel” (e.g. IT manager, facilities manager) in terms of their replacement or reconstruction cost, which is again translated to a scale value of 1-10. If software has its own intrinsic requirement for confidentiality or integrity (e.g. source code of bespoke software), it is valued in the same way as a data asset. Similarly implied asset values of physical assets and locations, which they acquire from their supported data and software assets (e.g. for higher

availability or confidentiality) are also calculated by the tool.

3.1.3. Threat and Vulnerability Assessment

In addition to asset values, the other two key components of a CRAMM risk analysis are levels (likelihoods of occurring) of threat and vulnerability. Threats and vulnerabilities are investigated against selected asset groups, which are put together to stay in reasonable review time frames. CRAMM has predefined tables for threat/asset group and threat/impact combinations. An exhaustive assessment of every threat to every asset group does not make sense and is not feasible, so the reviewer chooses here suitable threats and assets according to customer needs. On the vulnerability front, it should be noted that CRAMM is targeting a managerial level risk assessment, thus detailed technical, system specific vulnerabilities which may be identified by vulnerability scanners are not addressed by the tool.

There are two ways to assess threats and vulnerabilities: 'full' and 'rapid' risk assessment. In full risk assessment, which is mostly recommended, threats and vulnerabilities are identified by asking questions to support personnel (e.g. system or network administrators) from structured questionnaires and entering the answers in the tool, after which CRAMM calculates levels of threat to assets on a five point scale of "Very Low, Low, Medium, High or Very High" as well as levels of vulnerability to threats on a scale of "Low, Medium or High". The likelihood element is implied in the questions for assessing threats and vulnerabilities.

A well prepared and experienced reviewer may also use the rapid risk assessment, in which the threat and vulnerability levels are inputted directly into the system with a rating guide (e.g. "very low" threat for an incident "expected to occur on average no more than once in every 10 years", or "medium" vulnerability for an incident "occuring with a 33% to 66% chance of the worst case scenario realized") overruling the results from questionnaires. The qualitative approach here may currently be the only choice, since standards and relevant, reliable statistics on threats (except few surveys like annual CSI/FBI Computer Crime and Security Survey [CSI01]) or vulnerabilities are not available to produce accurate estimates on the regularity of them.

3.1.4. Risk Calculation

CRAMM calculates risks for each asset group against the threats to which it is vulnerable on a scale of 1 to 7 using a risk matrix with predefined values by comparing asset values to threat and vulnerability levels. On this scale, "1" indicates a low level baseline security requirement and "7" indicates a very high

security requirement.

The system can report the findings which should be presented to the management for agreement and approval to proceed to the risk management phase. At that stage a review meeting with the management should concentrate on major findings like high threat/vulnerability areas (which should be reviewed before for discrepancies –e.g. with “backtrack” facility of the tool- based on estimation or input errors), which also contributes to awareness.

3.2 CRAMM Risk Management

Based on the findings of the risk analysis, CRAMM produces a set of countermeasures applicable to the system or network which are considered necessary to manage the identified risks. The recommended security profile will then be compared against existing countermeasures to identify areas of weakness or over-provision.

CRAMM’s large selection of countermeasures (almost 4000) are collected together in groups and sub-groups, which have the same ‘security aspect’ like hardware, software, communications, procedural, physical, personnel and environment. They are also arranged in a hierarchical structure, being in three different categories, from high-level security objectives to detailed examples of implementation.

Each countermeasure is marked with the security level on a scale of 1 (Very Low) to 7 (Very High) which is selected by comparing the measure of risk. As a decision support for the management it is recommended to prioritize and report higher level countermeasures. One of the stronger points of CRAMM is assisting the prioritization by giving a countermeasure a higher priority if:

- it protects against several threats,
- it is required to protect a high risk system,
- there are no alternative countermeasures already installed,
- it is less inexpensive to implement (based on a general cost estimation),
- it is more effective to meet the objectives of its sub-group,
- it prevents an incident rather than detect or facilitate recovery.

This way one of the critics against this generation of tools, i.e. the ignorance of cost and efficiency evaluation of countermeasures while focusing on asset value, is covered by CRAMM to some degree (a traditional cost/benefit analysis is not offered, as regarded not applicable due to the intangible nature of risk).

The last activity in a CRAMM review is presenting to management a summary of

the findings and conclusions from risk analysis and explanation of recommended countermeasures providing a broad indication of the priority and costs involved in implementing them. The risk management report (like analysis report) can also be exported to Microsoft Word enabling organization-specific editing and formatting.

CRAMM does not include any detailed review of effective operation of countermeasures. Final choice to implement, enhance or remove countermeasures is the responsibility of management. Timing of the next review (recommended once a year) could also be agreed since business requirements, system configurations, threats and vulnerabilities would probably change.

CRAMM 'What-if' facility enables the user to assess the implications of the changes that have taken place, and the effects of different scenarios on the requirements for security. Besides several options in the tool to extract informational reports, a nested 'backtrack' facility provides reasons (threat, vulnerability and asset value) for recommending any one countermeasure to justify its selection.

When a CRAMM review has been completed the CRAMM software contains a complete database of the system or network reviewed, which can be used for configuration management and auditing. As a last remark, CRAMM does not require much resources, but a standard PC running Windows, and a hardware dongle for ensuring licensed use and protection of the often sensitive information collected.

4. Conclusion

CRAMM is a comprehensive tool for identifying security and contingency requirements, and justifying expenditure on necessary countermeasures especially of an IT operation.

The pluses of CRAMM are [GAM97], [CUS01],

- structured approach to risk analysis and management, based on well established method,
- assistance in contingency planning, BS7799 certification and audits,
- promotion of security awareness and acceptance,
- possibility of full reviews and rapid reviews (also allowing high-level reviews that support policy statements),
- regularly updated extensive hierarchical countermeasure database, covering also non-technical areas,
- relative prioritization of countermeasures, including effectiveness criteria and implementation costs,

- consistency resulting from similar solutions for similar risk profiles.

The minuses are [GAM97], [LAB99],

- need for qualified and experienced practitioners to use the tool,
- full reviews, which may last long with too much hard-copy output (which may be minimized by keeping the analysis at a required minimum),
- possible insignificance of some results in a full review due to delay between analysis and implementation after rapid changes to system or network reviewed.

The need for efficient risk analysis and management facing with ever growing challenges of the Internet and e-business era makes the use of tools like CRAMM indispensable. The organizations should however decide, preferably at the managerial level, for the best suitable way to go by evaluating their needs and requirements.

References

[BRE99] Brewer, Dr. David. “Risk, Security and Trust in the Open World of E-Commerce.” May 1999. URL: http://www.itsecurity.com/papers/p35.htm (22 March 2002).

[BRE00] Brewer, Dr. David. “Risk Assessment Models and Evolving Approaches.” IAAC workshop, London. July 2000. URL: http://www.gammassl.co.uk/topics/IAAC.htm (22 March 2002).

[CAI01] “CAIDA Analysis of Code-Red.” 15 August 2001. URL: http://www.caida.org/analysis/security/code-red/ (22 March 2002).

[CCC02] “Overview of Attack Trends.” 19 February 2002. URL: http://www.isalliance.org/resources/papers/attack_trends.pdf (22 March 2002).

[CHA99] Changduk, J., Han, I., Bomil, S. “Risk Analysis for Electronic Commerce Using Case-Based Reasoning.” 1999. URL: http://afis.kaist.ac.kr/download/inter_jnl012.pdf (22 March 2002).

[CHI97] Chisnall, W. R. "Applying Risk Analysis Methods to University Systems." EUNIS 97, European Cooperation in Higher Education Information Systems, Grenoble, France. 9-11 September 1997. URL: http://www.lmcp.jussieu.fr/eunis/html3/congres/EUNIS97/papers/022701.html (22 March 2002).

[COM02] “Computer Economics Security Review 2002.” URL: http://www.computereconomics.com/cei/news/secure02.html (22 March 2002).

[CRA98] Craft, R., Wyss, G., Vandewart, R., Funkhouser, D. “An Open Framework for Risk Management.” 21st National Information Systems Security Conference Proceedings. October 1998. URL: http://csrc.nist.gov/nissc/1998/proceedings/paperE6.pdf (22 March 2002).

[CSI01] "Financial losses due to Internet intrusions, trade secret theft and other cyber crimes soar.” March 2001. URL: http://www.gocsi.com/prelea/000321.html (22 March 2002).

[CST02] “CERT/CC Statistics 1988-2001.” URL: http://www.cert.org/stats/cert_stats.html (22 March 2002).

[CUG02] “About CRAMM.” URL: http://www.crammusergroup.org.uk/cramm.htm (22 March 2002).

[CUS01] CRAMM User Guide, Issue 2.0. Walton-on-Thames: Insight Consulting, January 2001.

[DOS01] “New Private-Sector Internet Security Alliance Launched.” 23 April 2001. URL: http://usinfo.state.gov/topical/global/ecom/01042303.htm (22 March 2002).

[GAM97] “A Practitioner’s View of CRAMM.” September 1997. URL: http://www.gammassl.co.uk/topics/hot5.html (22 March 2002).

[GIL89] Gilbert, I.E. “Guide for Selecting Risk Analysis Tools.” NIST Special Publication 500-174. October 1989. URL: http://csrc.nist.gov/publications/nistpubs/500-174/sp174.txt (22 March 2002).

[KRA99] Krause, M., Tipton, H.F., “Section 3-1: Risk Analysis.” Handbook of Information Security Management. December 1999. URL: http://secinf.net/info/misc/handbook/242-244.html (22 March 2002).

[LAB99] Labuschagne, L., Eloff, J.H.P, “Risk Analysis Generations – The Evolution of Risk Analysis.” August 1999. URL: http://csweb.rau.ac.za/deth/research/articles/ra_generations.pdf (22 March 2002).

[NIS91] “Description of Automated Risk Management Packages that NIST/NCSC Risk Management Research Laboratory have examined.” March

1991. URL: http://www.eff.org/Privacy/Newin/New_nist/risktool.txt (22 March 2002).

[OZI99] Ozier, W. “A Framework for an Automated Risk Assessment Tool.” 15 August 1999. URL: http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=228 (22 March 2002).

[SCO01] Hinton, C. “CRAMM.” December 2001. URL: http://www.scmagazine.com/scmagazine/sc-online/2001/review/059/product.html (22 March 2002).

[VEN99] Venter, H.S., Labuschagne, L., Eloff, J.H.P. “Real-time Risk Analysis on the Internet.” March 1999. URL: http://csweb.rau.ac.za/ifip/workgroup/docs1999/11_sec1999.doc (22 March 2002).