Elaborating quantitative approaches for IT security evaluation

Dimitris GRITZALIS, Maria KARYDA, Lazaros GYMNOPOULOS

Dept. of Informatics, Athens University of Economics and Business
76 Patission Ave., Athens GR-10434 Greece
tel. +301-8203505, fax: +301-8203507, email: {dgrit, mka, lazaros}@aueb.gr

Key words: IT Security, Information Systems Security, Evaluation, Certification Schemes, Complex for the Evaluation of Information Systems Operation Quality (CEISOQ)

Abstract: Information Systems security evaluation is a sine qua non requirement for effective IT security management, as well as for establishing trust among different but cooperating business partners. This paper initially provides a critical review of traditionally applied evaluation and certification schemes. Based upon this review, the paper stresses the need for an approach that is quantitative in nature and can address the problem of IS operational security. Then, such an approach is presented, mainly based on an existing complex of models (CEISOQ) for evaluating IS operation quality. It is argued that there are certain benefits if this approach is applied in combination with the traditional qualitative ones.

1. INTRODUCTION

Information Systems Security Evaluation has since long been one of the main areas of concern for people both in the academic and the industry field. Moreover, governments and state institutions, such as military bodies, have shown a great interest in the topic, resulting in the production of formal methods or approaches that have been also applied for commercial purposes.

Usual security evaluation approaches include some formal evaluation scheme, such as the Security Evaluation Criteria (TCSEC, ITSEC), the ISO 9000 series of quality assurance standards (BS 5750), the Code of Practice for Information Security Management (BS 7799), risk analysis and self-evaluation. Each one of these approaches suffers by some inherent drawbacks. All of them, however, focus on the design or a static aspect of the information system under evaluation, rather than on the system operation [8].

In this paper, we propose the use of a quantitative evaluation schema as an enhancement to current, mostly qualitative, security evaluation approaches. We argue that by combining qualitative and quantitative schemes we can evaluate both the static and dynamic aspect of an information system regarding its security niveau. In order to accomplish this, we propose the use of the "Complex for the Evaluation of Information Systems Operation Quality" (CEISOQ©) Mathematical Models, as a tool for evaluating IT security.

The paper is structured as follows: In Section 2 we present a review of currently applied security evaluation and certification approaches, as well as an outline of their main deficiencies. In Section 3 we emphasize the need for a combined approach and we argue for the need of a quantitative evaluation scheme to be used along with current approaches. In Section 4 we present CEISOQ and demonstrate the usefulness of applying it to the IS security evaluation area.

2. IT SECURITY EVALUATION APROACHES

Nowadays, the use of Information Technology (IT) infrastructure pertains all aspects of commercial activities. Most organizations rely on their IT infrastructure for their daily operations, as well as for gaining competitive advantage. Moreover, companies seek to form coalitions with their business partners, as a means of improving their position against the competition, resulting in the link of their IT infrastructure. Thus, organizations face the challenges of securing both their IT resources and their information, especially since the latter constitutes one of their valuable assets. This need brings the necessity of evaluating the IS security in the foreground.

In the first place, in order to decide on investing on IS security the decision-makers should have an estimate on the current level of security, as well as the level of security that will be achieved through this investment. Secondly, taking into the account that different companies interconnect their IS to achieve competitive advantages as previously described, a company should be able to prove to its business partners its capability in manipulating information in a consistent and secure way. In other words, it should be able to provide sufficient proof of the strength and efficiency of its Security Strategy, Policies and Controls. To provide this kind of proof and thus build the level of trust required among companies whose IS are interconnected, as well as to inspire confidence internally, two approaches are mainly used: evaluation and certification of their security schemes.

During recent years a lot of evaluation and certification techniques, models and schemes have been proposed in an effort to address the "confidence in security" issue. In particular four major techniques that can be directly linked to Information Systems Security have been proposed and subsequently used: the Security Evaluation Criteria schemes (TCSEC, ITSEC, CTCPEC, FC, CC), the ISO 9000 series of quality assurance standards (BS 5750), the Code of Practice for Information Security Management (BS 7799), risk analysis and self-evaluation. Each technique has its strong and week points [1].

2.1 Security Evaluation Criteria

The Security Evaluation Criteria, in all its forms, but particularly in its latest one i.e. the Common Criteria, is a tool for providing secure building blocks. These secure building blocks can be used to construct a secured Information System. This is a strong and, at the same time, week point. The evaluation and certification are totally focused on a certain well-defined Target Of Evaluation (TOE), which may be a product or a system, against a specific Security Target (ST) and thus are reliable as far as the specific security target is concerned, but it is very doubtful whether they can be applied on a TOE as wide and complicated as an Information System within the context of an organization [1, 2].

2.2 ISO 9000 and Code of Practice for IT Security Management

The ISO 9000 series of quality assurance standards address IT security indirectly. Nevertheless, they deal with some security related issues such as security policies, risk analysis, continuity planning, etc. The scope of ISO 9000 series of standards is the evaluation of processes and mechanisms rather than products or systems, in a way that certifies the ability of the company to provide products that meet customer's needs.

The Code of Practice for Information Security Management or the British Standard 7799 (BS 7799) is a security control reference document. It provides a detailed list of the available and most commonly used IS Security Controls. By using the Code of Practice a company can achieve baseline security and evaluate its security level by comparing against existing security controls [1]. Recently, BS 7799, with minor enhancements, became ISO standard ISO 17799. It is organized into ten major sections, covering topics that range from Business Continuity Planning and Physical Security, to Computer and Network Management and Asset Classification [11].

2.3 Certification Process

Should a company wish to comply with the security standards mentioned above and thus be able to provide concrete evidence that its products and/or processes satisfy a predefined set of security requirements, it must undergo a certain certification process. This process involves the company/organization requesting an independent third party (i.e. a Certification Body or a test laboratory accredited to perform the certification) to evaluate a certain product or process. The evaluation can last for a long period before resulting to certification, while also involving significant cost [7].

2.4 The self-evaluation approach

The self-evaluation scheme is what its name reveals. The organization performs by itself an evaluation of its own security controls and their effectiveness. Various techniques are employed by organizations in order to evaluate their security status, such as compliance to a baseline manual (Evaluation Criteria, Code of Practice, ISO standards etc.). Although self-evaluation schemes present certain advantages (i.e. low cost, ability to repeat the evaluation at short intervals), or whenever a change in the IS occurs, they remain highly subjective and their efficiency depends upon the skills and experience of the security personnel of the organization. Thus, their outcome cannot be exploited as a means to inspire confidence to business partners or customers.

2.5 Risk analysis

Risk analysis is the process by which an organization identifies asset values, threats and vulnerabilities. Risks are assessed in terms of potential impact that would be caused by the realization of a threat and need to be controlled or accepted. Risk analysis can be performed either officially, by a security consultant, or by the IT personnel conducting an analysis of information systems, thus minimizing the investment in time and resources. In the latter, baseline controls or a code of practice are often used to meet basic security requirements [9].

Risk analysis can be effective when conducted by an expert; however, it involves a certain degree of subjectivity, since it relies on the expert experience and competence. In addition, it involves considerable cost.

2.6 Shortcomings and deficiencies

The evaluation and certification approaches described above present advantages and drawbacks, several of which have been presented up to this point. We acknowledge the usefulness and necessity of certification schemes, as a basis for the formulation of coalitions of companies that are interconnected through their IT infrastructure, despite the high cost in terms of money and time.

We should not overlook, however, their limitation as evaluation tools. Information Systems (IS) comprise a set of components, namely hardware, software, processes, information and people, as well as the interaction among these components. Even if separate components have been officially evaluated (hardware or a software application) as to the security requirements they fulfill, this does not necessarily mean that the IS, within the specific context of the company resides on an equivalent security niveau. Moreover, none of the above evaluation and certification schemes take into account the actual IS operation. Certification schemes mainly depict the security level of the product-process design, neglecting interaction with other software, users, etc. The vast majority of these approaches fail also to provide company management with an evaluation tool to be used at the decision-making regarding security controls. We believe that investment on IT security should represent a certain part of the overall IT budget of company. However, such decision-making processes are often carried out by people, who are not experts on IT security, thus leading to problems when security-related choices or decisions have to be made.

We have so far argued that the evaluation and certification techniques described have strong points as well as weaknesses. Therefore, the adoption of any single one of them leaves security concerns not adequately addressed. A possible line of action could be the combination of some of these approaches.

3. A COMBINED QUANTITATIVE APPROACH

There is, therefore, a clear need for an evaluation approach, which:

i) Uses evaluation metrics, which are objective and can be substantiated.

ii) Can be exploited by management during decision-making.

iii) Involve all aspects of IS, as well as its operation.

iv) Is inexpensive and can be repeated as often as required.

v) Combines existing evaluation and certification schemes, in order to cover the need for certification and evaluation of IT security.

We argue that a quantitative evaluation approach, combined with some of the discussed ones, can meet the above requirements.

3.1 A quantitative security evaluation approach

The obvious advantage of a quantitative evaluation approach is, in the first place, the clarity of the numbers that come as results. The use of metrics allows comparisons to be done and different scenarios to be examined before a decision is reached. This means that both the experts and the non-experts can make their decisions and choices by using and comparing metrics.

Secondly, a quantitative approach provides the ability to express and therefore evaluate an IS as a less complicated and thus more coherent mechanism that obeys mathematical laws and can be dealt with in a more deterministic manner. Despite the fact that numbers cannot express adequately a complicated notion as IT security, they can be used as universal tools applicable in many different cases. Thus they provide a basis against which different controls can be evaluated, as to the security status achieved by implementing each set of them.

Thirdly, these metrics can be used to develop models, which can be applied again and again with different parameters in the same target of evaluation, providing us with useful information about the behavior of this target in different contexts. Finally, one can also resort to the literature for the importance of effective metrics [3,8], regarding IT security management.

4. IS QUALITY vs. SECURITY EVALUATION

The analysis of the term “information quality” results in different definitions, which include notions such as reliability, productivity, responsiveness, durability and accuracy [12]. On the other hand, “security” in general refers to one’s effort to protect his assets from potential threats. The most common use of the term security includes the protection of Confidentiality, Integrity and Availability of the assets as a whole [2]. The main objective of information security is the protection of these qualities of information, while information security and IT System Security compose IS Security. Security experts argue that this definition of IS security is not adequate in the modern environment and should include other notions as well, such as privacy, non-repudiation, etc. [5], in order to face a series of new threats.

In general, quality and security are related concepts [4]; consequently under certain constraints we can use Quality Evaluation Models for Security Evaluation. In the remainder of this paper we propose the use of an existing quality evaluation model, namely CEISOQ (presented in [6]), for the purposes of security evaluation.

4.1 CEISOQ

Modeling Software Tools Complex for Evaluation of Information Systems Operation Quality (CEISOQ) [6] is a set of mathematical models and their software implementation for the evaluation of the operation quality of IS. We propose applying CEISOQ for evaluating IS security for the following reasons:

- It is a qualitative approach.
- It takes into account the operational aspect of the IS.
- It covers all other aspects of IS security.
- It can be used in combination with other security evaluation schemes, such as risk analysis or self-evaluation.

4.1.1 Origin of CEISOQ

The development of CEISOQ stresses the need of organizations to make a successful selection in terms of cost, as well as efficiency and effectiveness, among a wide range of engineering solutions offered in the IT market. These solutions may meet user functional requirements but are not equally profitable for a certain company or group of users. The selection of the best solution is thus a difficult task and requires a set of appropriate tools. Such tools are models and methods that allow the evaluation, investigation and optimization of the basic IS Processes (information gathering, processing, storage, producing) [6].

Since such mathematical models pre-existed CEISOQ, the main objectives of this Complex include providing a universal model and a software tool for the evaluation of IS quality, the comparison of different IS engineering projects, the exposure of bottle-necks and the optimization of the basic IS Processes. Finally, CEISOQ allows for the simplification and expansion of other existing models [6].

4.1.2 Structure of CEISOQ

CEISOQ is composed of different mathematical models. Each model evaluates a specific IS operation in terms of compliance to user requirements, by feeding the models with input referring to them. In detail, each model is fed with figures as input and produces figures as output. The input figures are separated in two categories. Some of them express user requirements in terms of a required output and the rest express the attributes of the part of the IS under consideration. The output figure is used to determine the quality of the IS operation. This is achieved through the comparison of the output with the predefined required value. The Mathematical Models and their corresponding evaluated IS characteristics are shown in Table 1.

Table 1: *CEISOQ Mathematical models - Corresponding evaluated IS characteristics*

Evaluated IS characteristic	Model
1. Reliability of information producing	The model of information producing considering hardware, software unreliability
2. Timeliness of information producing	The models of calls processing
3. Completeness of output information	The model of Information System filling by data as regards new objects of application domain
4. Actuality of faultless information	The models of information gathering from source
5. Information faultlessness after checking	The model of input information check
6. Information faultlessness as a result of faultless users and staff actions	The model of users and stuff actions
7. IS protection against viruses influences	The model of computer viruses influences
8. IS protection against an unauthorized access	The model of an unauthorized access to information and software resources
9. Confidentiality of used information	The model of information confidentiality maintenance

4.2 Evaluating IS security with CEISOQ

In Table 2 we present how the *Complex for Evaluation of Information Systems Operation Quality* (CEISOQ) relates to IS security. It is clear from Table 2 that the mathematical models employed by CEISOQ can be useful for providing metrics for the evaluation of IS security, as it was defined previously.

Table 2. *Mapping CEISOQ quality characteristics to IS security attributes*

Quality characteristics evaluated by CEISOQ		IT Security attribute
	Reliability	Availability
	Timeliness	
	Completeness	Integrity
Actuality	Validity	
Faultlessness after checking		
Faultlessness of staff and users actions		
Protection against viruses		
Protection against unauthorized access		
	Confidentiality	Confidentiality

4.3 Combined qualitative approach for evaluating IS security

Most existing IS security evaluation schemes have something in common: their outcome is either the classification of their target according to a predefined scale or the accreditation of its conformance to a certain standard. Nevertheless, this does not significantly contribute to the improvement of IS security. The effectiveness of these approaches can be enhanced by applying a quantitative evaluation add-on.

In particular, we find that the CEISOQ evaluation models could be applied in circumstances, such as the selection of the appropriate set of security controls after a risk analysis has been carried out, or the evaluation of the operational security of the information system before complying to a certain baseline manual or security evaluation criteria. The application of this approach is facilitated by the fact that CEISOQ has been implemented as a software tool, available both for academic and commercial use.

5. CONCLUSIONS

We addressed the need for devising effective measuring instruments and methodologies in the realm of IT security management [3]. We reviewed a number of security evaluation approaches that are mostly employed, and showed why their use should be combined with the use of quantitative evaluation models.

We presented such a model, the “Modeling Software Tools Complex for Evaluation of Information Systems Operation Quality” (CEISOQ), and provided a mapping on how it can be exploited for the evaluation of IS security.

The main contribution of this paper to IT security evaluation is considered twofold.

- It argues for the need to combine current qualitative IT security evaluation schemes with a quantitative approach.
- It shows that evaluation tools and techniques, which can be useful for IT security evaluation, may reside in neighbor domains, (e.g. IS quality domain).

REFERENCES

[1] von Solms R. (1996), “Information Security Management: The Second Generation”, *Computers & Security*, Vol. 15, No 4, pp. 281-288.

[2] *Common Criteria for Information Technology Security Evaluation*, *(CCITT)*’, (1998), Version 2.0, CCIB-98-026

[3] Eloff M., von Solms S. (2000), ”Information security management: An approach to combine process certification and product evaluation”, *Computers & Security*, Vol. 19, No 8, pp. 698-709.

[4] Cooper M., Phillips R. (1997), “Killing two birds with one stone: Achieving quality via total safety management”, *Facilities*, Vol. 15, No 1, pp. 34-41.

[5] Parker D., (2001), “A note on our terrible security model”, *Computer Fraud and Security*, Vol. 4, pp. 18.

[6] Bezkorovainy M., Kostogryzov A., Lvov V. (2000), “*Modeling Software Tools Complex for Evaluation of Information Systems Operation Quality, CEISOQ*©”, SINTEG, Moscow 2000.

[7] Rannenberg K. (2000), "IT security certification and criteria: Progress, problems and perspectives", in *Proc. of the 15th IFIP Conference on Information Security (SEC-2000)*, Qing S., Eloff J. (Eds.), Kluwer Academic Publishers, China.

[8] Ortalo R., Deswarte Y. (1998), "Quantitative evaluation of information system security", in *Proc. of the 13th IFIP Conference on Information Security* (SEC-1998), Chapman & Hall, Denmark.

[9] Baskerville, R. (1991), "Risk analysis: An interpretive feasibility tool in justifying information systems security", *European Journal of Information Systems*, Vol. 1, No 2, pp.121-130.

[10] Ellof, M., von Solms, S. (2000), "Information security: Process evaluation and product evaluation", in *Proc. of the 16th IFIP Conference on Information Security*, Qing S., Eloff J. (Eds.), Kluwer Academic Publishers, China.

[11] The ISO 17799 Directory: Services and Software for ISO 17799 Compliance, ISO 17799 Audit, ISO 17799 Implementation and Security and Risk Analysis (also available at: http://www.iso17799software.com)

[12] Abdallah M. (1996), "An integrated approach for system evaluation: Study results", *Information Management and Computer Security*, Vol. 4, pp. 10-19.