INFORMATION SECURITY MANAGEMENT: THE SECOND GENERATION

R Von Solms
Port Elizabeth Technikon

Abstract

Information security has moved a long way from the early days when physical security, together with a set of backups, formed the backbone of a company's security controls. Today, information security is all about policies, standards, awareness programs, security strategies, etc. The aim of information security management efforts is to enhance confidence in the effectiveness of the information services within an organization. Unfortunately, this confidence is restricted to the organization itself and can only, with great effort, be passed on to external parties.

Today, business partners need to link their computer systems for business reasons, but first want to receive some sort of proof that the other partner has got an adequate level of information security in place. A security evaluation and certification scheme that can instill confidence and assurance, regarding information security status, to external business parties will solve a lot of problems for the commercial world.

This approach to Information Security Management, to proof adequate information security to external parties, is termed in this paper as; The Second Generation of Information Security Management.

Introduction

"We assume the bank will keep our money in a safe, use armoured vehicles for transport, only permit authorized people to complete a transaction, and audit all transactions. Furthermore, we require banks to adhere to accepted banking practices and open their books to independent review." [2] Doing this well may give one bank the competitive edge over its competitors, but more so, failing to do so may lose the bank valuable business. This latter case, i.e. failing to proof compliance to accepted practices, is a new phenomenon in the field of information security, but is growing to become a very important one.

Information security is moving very rapidly towards a stage, where proof of adequate security, to potential business partners, may help a company winning new business contracts, but on the other hand, a lack of information security may contribute to losing some business contracts.

The challenge of defining and introducing a security evaluation scheme that can certify an adequate security status, is termed in this paper as; *The Second Generation of Information Security Management.*

The objective of this paper is to;

- prove that the commercial world needs some information security evaluation scheme that can provide assurance to internal as well as external parties that adequate security controls are installed and
- to define a set of criteria which such a security evaluation scheme must satisfy to be successful.

In the rest of this paper, the evolution of information security will be addressed to provide some background information, a number of information security evaluation and certification techniques will be discussed, a set of criteria will be defined to provide a guideline for the definition of future, second generation security evaluation schemes and finally, a brief discussion on possible implementation schemes.

The Evolution of Information Security

Information security has been influenced largely on two fronts over the years; firstly, the scope of information security keep on expanding and secondly, the ultimate responsibility for information security has also moved over the years.

The Scope of Information Security

Information technology has advanced radically over the last thirty years and basically moved through three stages. Computing started with central mainframe computers in the 60's and only the information technology personnel had access to the facilities. From the middle seventies onwards; PCs, information sharing, departmental computing, local area networks, etc. were introduced. Many new, non-information technology personnel, were introduced to computers and computing, but all access to information systems were restricted to authorised employees within the boundaries of the organization. Today, many organizations want to embark on inter-company electronic trading and want to link their IT-facilities.

The scope of authorised access to information systems of an organization has expanded from within the computer room, to within the boundaries of the organization to outside the boundaries of the organization.

During these three stages, information security has moved from a situation where, a specially built room provided adequate security to all data processing activities, as it was called in those days. The operations personnel were mainly responsible for providing adequate security. They had to introduce some physical security controls, ensure that back-ups were made, that printouts were distributed in a secure way, etc. From the mid-seventies, just about every employee in the organization had access to some information systems and the information security blanket had to cover all of them. The scope of information security has thus expanded drastically, but was still restricted to the boundaries of the organization.

Although the scope of information security has changed over the years, the objective has always stayed the same. Information security controls were installed to minimise the chances of a threat having an adverse effect on the information or information services of the company, or to minimise the impact if something did happen. The objective of all the information security management efforts has always been, and still is, to provide *confidence* in the security of the information services of that particular organization. Many companies even perform a computer audit to provide assurance to their management that their internal controls are effective and efficient. All these efforts of information security management and computer audits, can only provide confidence or assurance domestically.

Today, as organizations want to embark on inter-company electronic trading, the information security blanket will have to expanded even further than company boundaries. Companies are afraid of linking their computer systems to Internet or the computer systems of a business partner, because of the possible security implications. Any organization would like to receive some or other *assurance* that other businesses have adequate control and security as well. [5]

The Responsibility for Information Security

In the s, information security was limited to physical security to a large extent. The operations manager was mainly responsible and the associated budget was very small. With the move of computing into the business areas, away from large central mainframes, information security concerns have not moved with the new distributed environments. Business management, in general, do not want to accept the responsibility for information security. This leaves the IT manager responsible for security on the business system applications on networks and main- or midframe computers. [3]

The responsibility for information security has at least expanded to another level, to that of IT management. Top management, who should actually be ultimately responsible for information security, because information is arguably the most precious asset of any organization, is in most cases not involved at all.

Top management is ultimately responsible for the well-being of the organization, and should thus accept the responsibility for information security. This has happened in some instances, but lack of top management involvement, is seen as one of the biggest drawbacks to obtain effective

information security in most organizations.

The responsibility for information security has moved through the years from the bottom upwards. Initially, the operations manager was responsible and later years the IT manager has accepted this responsibility. Maybe, this can be seen as one of the reasons why top management are reluctant to accept this responsibility, because they are use to delegate responsibility downwards and not to accept any responsibility coming from the bottom.

Top management sees their responsibility as; gaining market share, increasing product quality, investigating new business possibilities, etc. As soon as it become apparent that effective information security can give one company the competitive edge over the other, or winning new clients, top management will get actively involved. Otherwise, if it can be proved that the lack of information security was responsible for the loss of market share or the loss of potential new clients, top management will be forced to get involved and ensure that the information security situation improves. In both cases, once top management realizes that the well-being of their organization depends on their information security status, they will surely ask for some assurance that adequate security is in place.

On the other hand, in the cases where top management are actively involved, they increasingly demand assurance that controls are operating as intended, that the costly investment have generated real results. [5]

For many years, all information security management efforts were focused on providing an acceptable degree of confidence domestically, or *inwards*, in the information services of an organization. This can certainly be called the first generation of information security management and will definitely continue with great enthusiasm.

The dawn of the second generation of information security management has certainly arrived, i.e. to provide assurance or confidence of adequate information security controls to external parties, or *outwards*.

In both cases, whether inwards or outwards, the demand for assurance of adequate information security controls will increase. This assurance will be provided in the most effective way through an extensive security evaluation and certification scheme. The commercial world will welcome such a scheme with open arms.

In the next section, existing evaluation and certification techniques will be discussed. An attempt will be made to prove why none of them, at least in current form, can fulfil the role of providing outward assurance and confidence of information security controls to external parties.

Information Security Evaluation and Certification Techniques

A number of evaluation and certification techniques, models and schemes exist that can be linked to information security. The following will be discussed in more detail:

- Trusted Security Evaluation Criteria schemes,
- ISO 9000 (BS 5750), the leading international quality assurance scheme,
- The Code of Practice for Information Security Management (BS 7799) and
- self-evaluation.

Trusted Security Evaluation Criteria

The Trusted Computer Security Evaluation Criteria (TCSEC), first published in 1985, were the first criteria to achieve wide acceptance. They still serve as a yardstick for developing secure products. [4] The Information Technology Security Evaluation Criteria (ITSEC), published in 1990, and the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), 1993, were the European and Canadian answers to TCSEC respectively. An American reaction to ITSEC followed in 1992, by means of the Federal Criteria. Currently, all these parties are harmonizing these criteria and the draft Common Criteria are currently available for review.

Evaluation criteria refer to *products*, e.g. an operating system or *systems*, e.g. a collection of products assembled to meet the specific requirements of a given application. [4] Not all criteria mentioned above evaluate both products and systems, e.g. TCSEC, only evaluate products.

In all evaluation criteria, three aspects are addressed, i.e. *functionality* (the security features of a system), *effectiveness* (to ensure that the mechanisms used are appropriate for the given security requirements) and *assurance* (the thoroughness of the evaluation). TCSEC considers all three aspects simultaneously in the definition of its security classes, whereas ITSEC allows to address them independently. [4]

In the case of an ITSEC evaluation, a clear, definite *Target of Evaluation* (TOE) is defined. The TOE defines the product or system that need to be evaluated clearly. A *security target* is also defined for the system or product under evaluation. The security target specifies the security functionality of the TOE, i.e. what are the security objectives of the TOE. The TOE is then evaluated to ensure whether it satisfies the security target, and if successful, a certificate states that the TOE meets the security target.

These certified products and systems provide very secure building blocks towards a secure IT-environment, but do not in itself provide the secure environment. In the opening paragraph of this paper it was stated that one expects your bank to store your money in a safe. This in itself does not make the bank a good and trustworthy bank, even if the safe has passed all safety standards. A number of other procedural and documentational controls also need to be adhered to. Thus, as the very strong safe is only a building block towards a secure banking environment, an certified product or system is nothing but a secure building block towards a secure IT- environment. The evaluation process used in trusted security evaluation criteria is investigational to a large degree, that means that the product or system under evaluation is examined and tested. [4] A certificate of compliance is issued following a successful evaluation.

The ISO 9000 Series of Standards

The ISO 9000 Series of Standards is a series of international quality assurance standards, that apply to the quality management system and the process used to produce a product. [6] ISO 9000 establishes a basic set of quality system requirements necessary to ensure that the organization's process is capable of consistently producing products that meet the expectations of the customer. ISO 9000 does not address information security directly, but many security related issues are addressed by ISO 9000, e.g. security policies, risk analysis, continuity planning, etc. The ISO series of standards was published in 1987 and has been adopted by many countries and is rapidly replacing prior national and industry-based standards. The European Community (EC) has adopted ISO 9000 as its standards for quality assurance. This places a lot of pressure on all producers world-wide that wish to trade in European countries or even compete with European companies in other markets.

The ISO 9000 is a generic model for quality assurance in design/development, production, installation and servicing. The requirements of the standards have to be interpreted by each organization wishing to be registered formally as evidence of meeting its requirements. ISO 9000 makes use of an audit oriented evaluation method, which means that mainly documentation, procedures and processes are evaluated. ISO 9000 also issue a certificate following a successful evaluation.

Today, about 110 countries worldwide have accepted ISO 9000 as their quality assurance standards. It is estimated that about 100,000 companies are currently ISO 9000 compliant and the estimation is that by the turn of the century, 250,000 companies will be ISO 9000 compliant. [9]

ISO 9000 has taken off like a wild bushfire and the growth is forecasted to be exponential. Many organizations are ISO 9000 compliant purely for the marketing value of it. Many companies realize that their ISO 9000 certificate has won them contracts, non-ISO 9000 compliant companies find it more and more difficult to compete in the international market. The ISO 9000 certificates are used by companies to create confidence among their clients in their ability to deliver goods and

services that meets the clients requirements. [9] Top management of most modern companies know exactly what ISO 9000 is all about.

Code of Practice

The Code of Practice for Information Security Management is a reference document for managers and employees who are responsible for initiating, implementing and maintaining information security within their organization. [1] The objectives of the Code of Practice are; firstly, to provide a common basis for companies to develop, implement and measure effective security management practice and secondly, to provide confidence in intercompany trading. [1] The Code of Practice was published in 1993 and in 1995 a British Standard - BS 7799, based on the Code of Practice, was published.

The Code of Practice intends to serve as a single reference point for identifying the range of controls required for most situations encountered in industry and commerce. In today's world of increasing electronic networking between companies, it is good to have a common reference document. This common reference document provides an enabling mechanism for establishing mutual trust between networked sites and trading partners, and a basis for facilities management between IT users and service providers. [1]

A Set of ten categories, spanning the entire IT-environment, that are in general use in most companies are identified in the Code of Practice. Under each of these ten categories a comprehensive set of security controls are listed. Not all of these controls are applicable to every IT-environment and should be used selectively, according to local circumstances. "These generally accepted controls are often referred to as *baseline security controls*, because they collectively define an industry baseline of good security practice." [1]

If the Code of Practice is accepted by trading partners, inter-company trading will be able to be conducted on a more confident level if the trading partners know that their security controls are based on a common or similar code. Another advantage is that, once the concept of baseline security has been accepted, the basic principles, policies, standards, and procedures can be installed. No lengthy risk analysis or cost-benefit analysis is required. A further advantage is a clear statement of information security requirements also provides a yardstick for auditors. [3]

As, in the case with ISO 9000, the Code of Practice has been accepted with great enthusiasm. [5] The Code of Practice is currently being drafted into an ISO standard. No formal evaluation and certification scheme for the Code of Practice exists currently, but a certification and accreditation scheme for compliance to BS 7799 is under consideration in the United Kingdom.

Information Security Self-evaluation

Obviously, the ideal solution would be some IT security self-evaluation scheme. This is some scheme where the current installed information security controls can be evaluated by the organization itself to prove whether they have achieved adequate protection, or not. This will provide management with a checklist against which they can test their own current controls and approach in the area of information security.

Various organizations use various techniques and approaches to evaluate their own information security status. These techniques vary from pure 'gut-feel' approaches, where a very high level security screening is done, to more formal approaches where the information security status of the organization is 'measured' according to a definite methodology or against specific checklists.

Although self-evaluation holds many advantages, unless the criteria, to evaluate against, are well-defined with strict, definite conformance testing, the results will always be treated with some suspicion and will never be accepted outside the organization. This fact is underlined by the European Computer Manufacturers Association (ECMA) stating, "when criteria are ill-defined and ambiguous, any evaluation process (including one by a third party) will be arbitrary... and potentially very costly." [2] Self-evaluation can be very useful, but only for internal usage.

IT-Environment Security Evaluation and Certification Scheme

In the beginning of this paper, it was mentioned that an security evaluation and certification scheme, of an entire IT-environment, will be very useful to provide assurance of adequate information security controls installed to, firstly, own management and secondly, management of external parties.

Four techniques or approaches to IT security evaluation and certification were described in the previous section. None of them provide the ideal solution, but combining some of the strong points of each of them, may help to define the criteria for effective IT-environment security evaluation and certification scheme.

Trusted IT-products and Systems

Neither of TCSEC, ITSEC or the Common Criteria will provide the ideal evaluation scheme. Leon Strous commented [7] that security evaluation criteria are not only intended for application in the evaluation and certification of IT-products and systems, they must also contribute to an integral, consistent, analytical pragmatic and cost-effective approach to IT-security within the user environment. The focus of security evaluation criteria is currently on IT-products and systems. IT-systems and products only form part of a much broader IT-environment and this is really what need to be secured. The following quotation supports this statement, "it must however not be forgotten that the general issue is: the security of information and information processing, that supports the users main business process." [7]

From this, it can clearly be seen that security evaluation criteria, in its current form, will not be able to provide this comprehensive evaluation scheme that is envisaged. Although, it must be stressed clearly that ITSEC, TCSEC and, in the future, the Common Criteria will still provide the *secure building blocks* to help an organization towards information security in the entire IT-environment.

An alarming fact, that must be mentioned here, is that "few (if any!) commercial sites use products as they were evaluated." [2] This proves that the implementation and operation guidelines of trusted products and systems, need to be audited.

In the banking environment, mentioned at the start of this paper, the safe provides a secure storage place for money and other valuable articles. The fact that it is a very strong safe, and certified so by one or other standards institute, does not guarantee that the valuables and money stored in it is secure. The banking personnel must abide to some administrative and managerial procedures, e.g. who is allowed to have access to a key, where is the key stored, etc. Trusted products, e.g. a safe, do not provide security in it's own, but contribute to it, if the associated procedures are correctly followed.

From this discussion, the first criterium to a secure IT-environment can be formulated as follows:

> **Criterium 1: Trusted IT-products and systems, as evaluated and certified according to TCSEC and ITSEC, will not ensure a secure IT-environment, but will contribute to it as secure building blocks.**

The Technique of Evaluating an IT-environment

Charles Cressson Wood mentioned [8] that one of the biggest problems haunting information security efforts, are lack of an adequate infrastructure. With this he means; policies, procedures, responsibility statements and related matters. This is precisely the advantages of ISO 9000. The establishment of a concrete organizational structure, clear definition of responsibilities, improved quality of communication and internal information, maintenance of up-to-date systems documentation, better control over organizational and system growth, formal problem management and resolution process, and standard processes for training workers. [8] This view is supported by Leon Strous, who commented that current security evaluation criteria fall short on their ability to real-life environments. According to him, the key words to security in real-life IT-environments are 'administration' and 'organization'. [7]

ECMA [2], further underlined this point, by stating: "our recommendation is to look to an existing quality program, where ISO 9000 seems to be the leading international contender, to fulfil the need for security evaluations." Information security specialists will receive more of top management's attention if they make more use of the ISO 9000 approach. [8]

In our banking example, strict organizational and administrative procedures are defined and practised for the execution of all transactions and tasks, and all these banking practices are reviewed and audited.

From what was mentioned in the previous paragraphs, and if one looks at the support that ISO 9000 received from top management around the world, then a similar audit oriented approach to information security seems to be a definite answer. The second criterium to a secure IT-environment can thus be formulated as follows:

> **Criterium 2: An audit oriented evaluation approach is needed to ensure that all IT security policies, procedures, functional and related issues, within the IT-environment, are introduced and practised as prescribed.**

The Scope of the Evaluation

As the Code of Practice becomes more popular, many organizations will want to be seen to comply with the Code of Practice. Positive assurance are thus needed that the necessary compliance procedures and systems are in place, and that they are correctly operated. [5]

The Code of Practice addresses some of the shortcomings identified earlier, e.g. all of policies, organizational structure, responsibilities, administrative procedures, etc. are addressed in the Code of Practice. The entire IT-environment can thus be included in the evaluation process, and not merely isolated products and systems. Further, the Code of Practice provides a clear yardstick for auditors and the security baseline is a useful parameter against which to conduct an audit. [3] At this stage all Code of Practice audits, for compliance to the Code of Practice, are largely limited to internal audits, thus for self-assurance. Some consultants do perform audits at one company and then provide the necessary assurance of compliance to another company, that require the necessary assurance, and visa versa.

The Code of Practice addresses ten categories, these are [1]:

- security policy
- security organization
- assets classification and control
- personnel security
- physical and environmental security
- computer and network management
- system access control
- system development and maintenance
- business contingency planning
- compliance

According to the authors of the Code of Practice, these ten categories cover the entire IT-environment that would require any baseline controls. This IT-environment, as referred to in this context, can be either an entire organization or a subset that can be properly delimited for this purpose. Typical delimitations would be either organizational (a division, a business area, etc.), geographical, or both. [5] Any IT-environment evaluation should cover all aspects within an entire environment. Criterium three can thus be formulated as follows:

> **Criterium 3: The evaluation scheme should span an entire IT-environment and should not be restricted to isolated products and systems.**

Levels of Security

The Code of Practice suggests the baseline security controls that should be in place in most organizations. In some cases, stronger controls, outside the scope of the Code of Practice, may be required. [1] The Code of Practice only addresses baseline security controls, which represents the minimum. Whether this minimum will satisfy all trading partners, is an open question?

This identifies another very relevant aspect, i.e. what level of security is needed and/or acceptable? Surely, this will differ depending on circumstances and from one situation to another. Both TCSEC and ITSEC introduced different levels of security, e.g. C1, C2, B1, etc. One the other hand, ISO 9000 and the Code of Practice utilizes a binary approach, i.e. either compliant or not.
The ideal evaluation scheme, should make provision for more that one level of security. This will enable some companies, that require more stringent controls than prescribed in, for example the Code of Practice, to get evaluated and certified as such.

Criterium 4: The evaluation scheme, should make provision for more than one level of security.

Self-evaluation

At this stage, most Code of Practice audits can be classified as examples of self-evaluation. The definite set of criteria defined in the Code of Practice makes it possible. Some software packages already exists to help an organization in this self-evaluation process of compliance to the Code of Practice. Gary Hardy [5] also calls for clear standards and criteria against which controls can be evaluated, "one harmonised set for both auditors and IT professionals".

Although self-evaluation depends on very strict and definite criteria, the results will in most cases be queried by a second party. The criteria, no matter how precisely defined, will always be open to some interpretation that could lead to some subjectivity. Not withstanding that, the results from a self-evaluation exercise will always be very useful internally.

Criterium 5: The standards and criteria defined need to be precise enough to enable self-evaluation, for domestic use.

In this section, a set of five criteria has been motivated and defined that should feature in any IT-Environment Security Evaluation Scheme. Such a scheme will play a prominent role in the second generation of information security management, where assurance of sound information security practices can be produced to management, both internally and externally.

Conclusion

Many companies are becoming aware of the increasingly importance of information security. In many of these companies, top management are actively involved, but in many companies this is not the case. In the era where inter-company electronic trading is taking off, the security status of business partners is a real point of concern. A definite need exists for companies to provide the necessary assurance, that adequate information security controls are in place, to either own top management (internal) or to concerned management of potential business partners (external).

After studying different evaluation and certification schemes, a set of five criteria has been defined that should form part of such an IT-Evaluation Security Evaluation Scheme (IT-ESES).

These criteria can be summarized in a definition for IT-ESES:

An audit oriented evaluation and certification scheme that evaluates all relevant aspects, e.g. organizational, managerial, administrative, functional, etc., in an IT-environment, that possibly utilizes trusted products and systems, and that utilises clearly defined criteria that will enable self-evaluation.

As mentioned before, the Code of Practice is currently being considered by ISO/IEC JTC1 SC27 as an international standard. A certification scheme for compliance the BS 7799 (the U.K. standard based on the Code of Practice) is currently under consideration. It is thus very premature to think of an international certification scheme for the Code of Practice, but that will certainly be a bold step in the right direction. Such an evaluation and certification scheme may sound very impossible at this point in time, but this is what the commercial world wants. "Aim for the sun and you might hit the moon."

References

[1] *Code of Practice*, PD 0003, BSi, Sept 1993.

[2] **European Computer Manufacturers Association**, *Secure Information Processing versus the Concept of Product Evaluation*, ECMA TR/64, Dec 1993.

[3] **Fitzgerald K.J.**, *Information Security Baselines, Information Security & Computer Security*, MCB University Press Ltd., Vol 3, No 2, 1995.

[4] **Gollmann D.**, *Lecture Notes on Evaluation Criteria*, Royal Holloway, University of London, Jan 1996.

[5] **Hardy G.**, *Promoting Computer Security through Possitive Computer Audit*, Compusec '95, Oct 1995.

[6] **Schmauch C.H.**, *ISO 9000 for Software Developers*, ASQC Quality Press, Milwaukee, Wisconsin, 1994.

[7] **Strous L.**, *Security Evaluation Criteria*, Computers & Security, Vol 13, 1994.

[8] **Wood C.C. and Snow K.**, *ISO 9000 and Information Security*, Computers & Security, Vol 14, 1994.

[9] SEAL, University of Witwatersrand, South Africa.