From Trusted Information Security Controls to a Trusted Information Security Environment

ROSSOUW VON SOLMS AND HELEN VAN DE HAAR
Port Elizabeth Technikon South Africa

Key words: Information security controls

Abstract: To protect the information systems of an organisation an appropriate set of security controls needs to be installed and managed properly. Through a risk analysis exercise, the most effective set of controls is recommended. This analysis or identification process can be subjective and many assumptions are made about the environment. A possible solution may be the definition of suitable protection profiles that will include the best suitable security controls for specific information technology environments. This paper will provide some guidelines in the formation of a fully defined security control. Sets of these controls can be used in the determination of an information security profile that will encompass all aspects of security such that no assumptions need to be made, thereby leading towards a totally secure organization.

1. INTRODUCTION

Risk analysis has traditionally been the dominant technique to identify and assess risk levels within the various business areas in an organization. From this assessment, a set of security controls is proposed to provide adequate security within the different business areas. Unfortunately, this technique is quite complicated and resource intensive, with the result that many organisations do either nothing or bypass risk analysis and propose and implement security controls based on ad hoc thoughts. The result is that many high risk areas may be under protected or vice versa. According to the information security survey (Department of Trade and Industry, 1996), most small to medium sized organizations do not perform a risk analysis. Possible

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35515-3_53

S. Qing et al. (eds.), *Information Security for Global Information Infrastructures*

reasons for this are: firstly, usually most small to medium sized organizations do not have the required expertise to conduct a proper risk analysis and cannot afford the services of a consultant and secondly, the awareness of information security is usually very low at these organizations. A relative new development has been the establishment of information security baselines, an approach that suggests a minimum set of security controls that should be installed under most circumstances. Thus, any organization can obtain a minimum level of protection that should be adequate under normal conditions without going through an expensive risk analysis exercise. This is obviously not the ideal solution, but much better than ad hoc or absolutely no control. A number of security baselines manuals have been developed over the last few years, of these baselines, the British Code of Practice for Information Security Management (Code of Practice for Information Security Management, 1995), and German IT Baseline Protection Manual (IT Baseline Protection Manual, 1995) are probably the best known. Obviously, all these manuals propose a very extensive set of security controls and an organization must identify which of these controls are applicable to their unique situation and level of risk. This identification process can become very detailed and result in a complete detailed risk analysis, thus losing the advantages of such security baselines. An alternative would be to establish a number of different subsets of controls, based on specific criteria. These subsets can be termed protection profiles, applicable to specific circumstances or situation. A specific organization will thus merely select the most appropriate protection profiles, which will spell out precisely the security controls included in the profiles, and make assumptions about the surrounding environment. The rest of this paper will suggest an information security profile, encompassing all aspects of security in the organisation.

2. TRUSTED CRITERIA FOR PRODUCTS AND SYSTEMS

In 1983 the United States published the Trusted Computer Security Evaluation Criteria (TCSEC) commonly known as the Orange Book (Department of Defence, 1985). In 1990 the European Commission announced the Information Technology Security Evaluation Criteria (ITSEC), or the White Book (Information technology security evaluation criteria, 1990). The objective of both these sets of criteria was to evaluate software products and systems as being "secure". TCSEC only evaluates products that can be bought "off the shelf", for example: Windows NT, UNIX, etc. Everyone that buys that particular evaluated product, can be

assured that the product meets the predefined security evaluation criteria, thus a certificate for technical security is implied. ITSEC, on the other hand, evaluates products as well as systems, for example: a pay-roll system running under a specific version of the Oracle database on some version of the UNIX operating system. The whole bundle of products and systems can be evaluated together to ensure a very secure unit. TCSEC and ITSEC certify that a specific set of technical security controls is present in the product or system and that it has been installed correctly. Different levels of certification exist and an organization must determine for themselves which certified level of security will be adequate for their specific risk level. No guidance is given to any user as to which certified level of security is best for which type of operation.

As far as individual organizations are concerned, using TCSEC and ITSEC evaluated products and systems will not ensure secure operating environments, but will surely contribute to it. The following two quotations from ECMA will highlight this point: *"The usage of evaluated products within a system does, however, not necessarily mean that the whole system is secure."* and *"Few (if any) commercial sites use products as they were evaluated."* (European Computer Manufacturers Association, 1985) Therefore, evaluated products and systems provide a secure computing base, but are not the sole solution to secure computing environments. Technical security mechanisms need to be augmented by proper operational procedures to be effective.

3. SECURITY BASELINES

Security baselines are a well-established concept that has won much support lately. Baselines can be seen as a bottom-up approach, where a generic set of controls is defined for most organizations or business areas under normal circumstances. By installing these baseline controls, an organization can be sure that the most common and serious risks have been addressed adequately under normal, generic circumstances. It must be stressed clearly, that the objectives of security baselines are to provide the minimum level of security.

Security baselines do augment evaluated products by addressing both technical and operational issues. Some baseline manuals include an extensive set of controls, covering all possible areas that need to be protected. One of the problems associated with security baseline catalogues is the lack of guidance on which of the controls are applicable to that specific organization or business area under consideration.

4. BASELINE PROTECTION PROFILES

In some disciplines, like finance and health, specialised baselines exist that address risks specific to those disciplines. These disciplines have some guidance on which controls are required for their specific disciplines with their unique risks associated. These discipline specific baselines do not make provision for specific environmental or personnel risks. Thus, although these baselines may address discipline specific risks, they cannot cater for every unique situation as far as environmental, hardware, software, personnel, communications, etc. risks are concerned.

TCSEC prescribes a specific set of controls to be present and correctly installed for every level of security certified. Each of these levels provides a specific generic protection profile. If one requires a high level of protection, an appropriate 'protection profile' is chosen or if not such a high level of protection is required, a different 'protection profile' is chosen. But, as highlighted earlier, TCSEC does not cover all aspects, associated with information security, comprehensively. These 'protection profiles' prescribed by TCSEC need to be expanded to cover beyond hardware and software. Operational, managerial and administrative controls also need to be included in these protection profiles. Further, these protection profiles also need to take various combinations of operating environments, systems, disciplines, environmental factors, etc. into account.

5. COMMON CRITERIA PROTECTION PROFILES

The Common Criteria (CCITT) (Common Criteria for Information Technology Security Evaluation, 1998) provides a protection profile which contains a set of security requirements for a set of Targets of Evaluation (TOEs), that will comply fully with a set of security objectives. A Target of Evaluation can be an information technology product or system that is to be evaluated together with its associated administrator and user guidance documentation. There are associated hardware, software and firmware security functions of the TOE that must be relied upon for the correct enforcement of the TOE.

The Common Criteria can be used by consumers, developers and evaluators in different ways. Developers, for example, use the Common Criteria construct called a Security Target (ST) which can be used to identify security requirements that must be satisfied by the developed product or system. Evaluators will judge if an existing product or system (i.e. a Target of Evaluation), conforms to its security requirements. Consumers, on the other hand, use the results of the evaluation of a TOE, in order to make a

decision as to whether that evaluated product or system, fulfils their security needs. This is also done by means of the Common Criteria protection profile that can be used by the consumers as a structure in which to express their specific security requirements for information technology security measures in a TOE.

Besides the assets requiring protection, the Common Criteria protection profile has to consider the relevant security aspects in the physical environment around the TOE, as well as the purpose of the TOE, in other words, the type of product and intended usage of the TOE. Based on these considerations, certain statements are made about the TOE, including assumptions to be met by the TOE environment in order for the TOE to be considered secure.

A protection profile can therefore be used by the Common Criteria to describe a baseline protection mechanism for a TOE, and the level of this baseline protection mechanism is not necessarily chosen to be the minimum protection possible, but rather scaled to suit the TOE. It can also be seen that the Common Criteria protection profile makes necessary assumption statements about the TOE environment, perhaps related to personnel and physical security aspects. These assumptions should not have to be made, but rather, some security profile should be in place to remove the need for assumptions.

6. INFORMATION SECURITY PROFILES

An information security profile for an organization should not be required to make assumptions about environments, because even human behaviour can be monitored, for example by techniques such as ISO9000. Such an information security profile should define precisely which controls are required, and each control should include all aspects of security. One can look at various issues surrounding a control, to decide when it is a "complete" control, fully capable and totally trustworthy. For the purposes of the analysis of a "complete" control, an example of a door lock can be used. The aspects associated with a control can then be defined as follows:

Control Aspect #1: How strong is the control? The first question that one should try to answer is how strong the control is, and in the example, one looks at the strength of the door lock as a technical control for securing a door. The "control strength" aspect, for the purposes of our definition, is determined independently of the environment in which it is intended to be implemented, i.e. local influences need not be taken into account and will be dealt with in another definition further below. This aspect simply determines the strength of the

individual control as far as functionality is concerned. For example, a lock that has been tested and certified by the SABS (South African Bureau of Standards) can be accepted as being a strong lock.

Control Aspect #2: Has the control been installed correctly? Assuming that an SABS lock is required and in place, one should also ensure that the lock has been installed correctly according to installation specifications, and if need be, by a reputable locksmith. The lock will not work efficiently if it is installed on the wrong side of the door or in the wrong place. This control is also independent of the environment for which it is intended, and is only concerned with the correct installation of the individual control. A strong lock that has been installed incorrectly will definitely not provide the required protection.

Control Aspect #3: Is the control sufficiently capable of doing the job? It should be clear whether the lock is enough to secure the door. If not, then another control should be identified and installed to provide the required level of protection. For example, if a single bank note is lying inside the room behind the locked door, and a lone thief is standing outside, then the lock may be strong enough to deter the thief. However, if the room contains a few million bank notes and a syndicate of armed robbers is waiting outside the door, then the lock is insufficient and should be supplemented with additional controls. This control aspect, therefore, is dependent on the environment in which the control is intended to be implemented.

Control Aspect #4: Are there operational rules governing the functionality of the control? Operational rules and guidelines will govern the correct usage of the control, ensuring maximum functionality. For example, there should be a rule stating that the door should be kept locked at all times when not used for thoroughfare and that the keys should be stored in secure locations. Rules are necessary for the maintenance of the lock as well. There should be rules for corrective action, should there be any deviance from these rules. This control aspect is definitely dependent on the environment in which the control is implemented.

Control Aspect #5: Are checkups made on the control? Operational rules may be applied as in control aspect #4, but there must be a way to determine deviance from these rules. For example, the lock may be in place, having been installed correctly, and it may be strong enough to keep the door locked. There may be rules in place to ensure the correct usage of the lock at appropriate times, but are these rules enforced? Checkups by means of evaluation and certification exercises, should be done to ensure that the control is

being used correctly and is maintaining its functionality and should also take into account the changes in the environment which may require a different strength for the control. This should be done at regular time intervals. For example, the parent in the house should check regularly that the lock is fully functional and capable, and that the children are obeying the rules for keeping the door locked. This control aspect is also totally dependent on the installed environment.

At this stage, with all the enveloping aspects of the control in place as suggested, the control can be accepted as being completely trustworthy because:

- It is strong enough,
- It has been correctly installed,
- It is applicable to the intended usage,
- It effectively keeps everyone out when applied,
- It is governed by rules for installation, usage, effectiveness and maintenance and
- It is monitored regularly for all of the above.

If these aspects are all present in a control, one can trust that the control will provide a prescribed level of protection to the assets it is intended to protect. The next important question is: which set of controls will be best suited to a specific defined environment? The modern trend in selecting security controls, is to identify comprehensive sets of controls and to select the most appropriate ones, using one or other selection method.

One method is to use a many-tiered structure, allowing levels of controls, the top level being the information security baseline requirements which should be implemented in all organizations, the next level being devoted to more discipline specific groupings (e.g. medical), and a third level for the level of security required, for example, low, medium, high and so on. On the other hand, a network structure with many entry and exit points, may be preferable due to the diversity of organizations. A hierarchical-type structure, instead, could provide adequately for "inheritance" of protection from higher layers. For example, if at a certain level, a control does not include a particular environmental protection mechanism, perhaps it is already defined at a higher level, thereby implying its encompassing protection for all sub-level controls. Whatever, the proposed model will be, it will have to represent the complete picture of an information security profile, which can be used for any and every organization. By careful navigation of an implementation of the model, one should arrive at the full representation of all applicable security requirements, thereby achieving the total suggested implementation of the information security profile for the organization.

The clever integration of principles from trusted criteria, protection profiles, security baselines and discipline specific security baselines will provide the foundation on which such a model for an information security profile will be based.

7. CONCLUSION

The Baseline method for providing information security in an organization is easy to apply yet will not cater for all levels of security required in any organization, because it is aimed at providing for a particular, usually minimum, level of protection. The Common Criteria protection profile makes assumptions about the environments of the products or systems being evaluated. A method is required, whereby organizations can derive the total set of controls for information security, without having to make assumptions about various environmental issues like personnel behaviour. Some research is being done to provide a model for an information security profile which can be implemented in an organization without requiring assumptions to be made about various controls. The model will make use of controls that are fully defined and that cover all aspects of security. This paper is a report on the progress made so far in defining such a model for an information security profile.

REFERENCES

Department of Defence (DoD). (1985). Department of defence trusted computer system evaluation criteria. Washington D.C.

Information Technology Security Evaluation Criteria (ITSEC). (1990). Harmonized criteria of France, Germany, the Netherlands and the United Kingdom.

European Computer Manufacturers Association (ECMA). (1985). Secure information processing versus the concept of product evaluation, TR/64, Dec. 1995.

Code of Practice for Information Security Management (CoP) BS7799. (1995). British Standards Institute. PD0003, United Kingdom.

IT Baseline Protection Manual (ITBPM). (1995). GISA, BSI, Germany.

Common Criteria for Information Technology Security Evaluation (CCITT). Part 1: Introduction and General Model, Version 2.0, CCIB-98-026, May 1998.

Department of Trade and Industry. (1996). The Information Security Breaches Survey 1996. United Kingdom.