Information security management: why standards are important

Rossouw von Solms
Department of Information Technology, Port Elizabeth Technikon, Port Elizabeth, South Africa

Keywords
Certification, Computer security, Data security, Evaluation, Information management, Standards

Abstract
Information security is no longer a domestic issue. In this age of electronic commerce, one company's information security certainly affects their business partners. For this reason it became imperative that business partners demand an acceptable level of information security from one another. Information security management standards should certainly play a major role in this regard. In this paper, some information security management standards and their applicability will be discussed and put into context.

Information Management & Computer Security
7/1 [1999] 50–57

[ISSN 0968-5227]

1. Introduction

Information technology (IT) has become part and parcel of the business world today. In fact, it will continue becoming an ever larger factor in the future. Organizations will interlink their IT systems as a result of linking to the Internet, EDI, EFTPOS, etc. All of this may hold an information security risk for an organization. Organizations attempt to secure their own IT environment, but they have little control over the IT systems with which they link. If those external IT environments are insecure, they may pose a threat to the IT systems in the host environment.

Information security is no longer only a domestic issue, but it affects external parties as well. It can be detrimental to an organization if its business partners, or potential business partners, label that organization as insecure, as far as information protection is concerned. This previous statement can best be explained by means of an example. This example will then gradually be put into context, as far as information security is concerned.

Driving the only motor vehicle on a farm requires very little safety and traffic regulations and it is fairly easy to drive safely around the farm. The only requirements will be some technical safety mechanisms in place and satisfactory working order, for example brakes, safety belts, etc.

If more than one motor vehicle is used on the farm, a number of additional rules and regulations need to be introduced, for example, driving on either the left-hand side or right-hand side of the road, stopping at intersections, etc. Many of these newly introduced rules and regulations are procedural of nature and are independent of any technical safety mechanisms.

When a driver drives on public roads, a totally different approach to road safety is introduced. One reckless driver poses a big threat to other vehicles and their drivers. Although the technical safety mechanisms are very important, the emphasis is placed mainly on the rules and regulations of safe road usage, for example, the correct usage of direction indicators, etc. A number of other features are also introduced, for example, a driving licence is required for every driver, motor vehicles are tested to ensure that they are roadworthy, traffic officers are on duty to ensure that all technical safety mechanisms are in working order and that all procedural regulations are adhered to, etc. To drive on the open, public road requires a totally different approach to safe driving, with the introduction of many procedural rules and regulations, that need to be controlled by an independent authority.

In the rest of this paper, an analogy between this example and the computing world of today will be drawn.

2. The evolution of information security

In the early computing days, mainframe computers with single processors were used. Only one program was executed at a time, no shared databases existed, no memory had to be shared, etc. To secure such an environment was easy. A few technical and physical mechanisms were adequate to secure the complete information processing environment. This era can be compared with being the only motor vehicle driver on a private farm road.

The PC revolution and multi-processing computer systems resulted in a number of additional technical security mechanisms, for example, user identification and authentication, memory clearance, access control to data, etc. To provide adequate information security to this environment, more technical and also procedural security mechanisms were required, as was the case with more than one motor vehicle driver on a farm. The important factor during this era was that the complete IT environment could be controlled and secured, to a satisfactory level, by its

Information Management & Computer Security
7/1 [1999] 50–57

own personnel. An information security policy spelled out to the personnel what was allowed and what not. This information security policy was an internal set of rules and regulations and adherence to this policy was controlled within the organization, by its own personnel.

As organizations link their computer networks to the Internet or to the IT networks of business partners, central control over their IT systems and users, and thus information security, can be lost to a large extent. The information security policy, which dictates the behaviour of users within an organization, has no influence on any users outside the boundaries of the organization. To ensure a secure IT environment, under these circumstances, it is required to have a secure IT community. A set of rules and regulations for all users will have to be introduced and some authority will have to see that all parties adhere to this. In terms of our example, driving on the public road requires a legal driving licence, which implies that the driver knows, accepts and promises to adhere to the rules and regulations of driving on a public road in that country or state.

To expect that all Internet users must adhere to an international set of IT user regulations is obviously not possible, but no country merely accepts the driving licence of all other countries. To expect one's business partners to obtain and adhere to an "IT driving licence" is possible, and only those organizations will be allowed to link to one's IT systems. To define the contents of an international information security policy and an associated set of security controls is one problem, to enforce it may be an even bigger one. This challenge has to be overcome, because many organizations are already, and most will soon be, embarking on the road of electronic commerce. If an organization is found secure enough by others, it will be welcomed to join, if not, it may be excluded and left in the cold. A practical example is that of a large, well-known retail group in the UK that communicates only through electronic means with all its suppliers. Nobody can supply any goods to this retailer if it is not done electronically, but before any electronic links are established, the supplier must prove to the retailer that it meets the *Code of Practice for Information Security Management*, a British standard (BS 7799) for minimum information security practice. This Code of Practice will be discussed later in this paper.

This discussion proves that in the era of electronic commerce, proper information protection, and proof thereof, may be demanded among business partners. Surely technical protection mechanisms will always play an important role in securing an IT-environment, but proper administrative and managerial controls, to help dictate the actions and behaviour of the users, will play a very important role in future secure IT-environments. The whole process of being evaluated and certified as secure, is a reality and international initiatives are well under way in this regard.

As proven by the example earlier, technical security controls alone cannot enforce a secure IT environment, it needs to be supported by proper operational controls. These operational controls will dictate the actions and behaviour of users when working with information. This combination of technical and operational controls may result in a secure IT environment.

Before anyone can take his/her motor vehicle onto a public road, a certificate must be obtained to prove that all the technical security aspects of the vehicle are functioning satisfactorily. Similarly, the basis for secure computing is a certificate for secure technical functioning of the computing base. This aspect will be discussed in the next section.

3. Technical security

In 1983 the USA published the *Trusted Computer Security Evaluation Criteria* (*TCSEC*), commonly known as the Orange Book (Department of Defense, 1985). In 1990 the European Commission announced the *Information Technology Security Evaluation Criteria* (*ITSEC*, 1990), or the White Book.

TCSEC only evaluates technical security features of 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 payroll 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.

During evaluation, three independent factors are scrutinized. These are:

1 functionality, i.e. the security features of a product or system;
2 assurance of correctness, i.e. the thoroughness of the evaluation; and
3 assurance of effectiveness, i.e. are the security mechanisms used appropriate.

These factors can be explained better by means of another example.

Example:
If I want to secure my house, three factors need to be considered. First, I need to identify some functional security mechanisms to introduce or install at my house, like door locks, burglar bars, electronic alarm system, etc. Second, I need to be assured that these security mechanisms are properly installed and will function correctly and third, that the set of security mechanisms is appropriate and effective enough to provide the level of security required.

TCSEC and ITSEC differ in the way they apply these three factors. TCSEC consider all three factors together, whereas ITSEC handles functionality independently and assurance of correctness and effectiveness together. This will again be explained by means of the example.

Example:
Let us imagine four different levels of household security; levels 1 through 4.

The functionality for each of these four levels are dictated by the following security mechanisms:

- level 1 – no security mechanisms;
- level 2 – door locks at all doors;
- level 3 – door locks at all doors and burglar bars;
- level 4 – door locks at all doors, burglar bars and an electronic alarm system.

The assurance of correctness for each of the four levels are dictated by the following increasing levels of trust:

- level 1 – none;
- level 2 – door locks must be installed by the builder;
- level 3 – door locks and burglar bars must be installed by a security company;
- level 4 – door locks, burglar bars and electronic alarm system must have a South African Bureau of Standards (SABS) certificate and must be installed by a security company.

It is clear that as the functionality increases from one level to another, the security mechanisms become more and more stringent. Similarly, as the assurance increases from one level to another, the trust in the security mechanisms also increase.

TCSEC defined a number of functional levels and identified appropriate security mechanisms for each of them. Similarly, for each of these levels, increasing assurance is also defined. TCSEC will evaluate a product for a specific level of security and both the functionality and assurance must meet the criteria set for that level of security. TCSEC will not evaluate a product for functionality level 3 and assurance level 2. If a product is evaluated for a specific level of security, both functionality and assurance will be evaluated on that level. If, in the example, a house is successfully evaluated for level 3 security, one can assume that the security feature of the house will include door locks and burglar bars and that it was installed by a security company.

ITSEC on the other hand does things differently. ITSEC does not predefine functional security levels. No security mechanisms are thus identified and dictated to specific functional levels. A number of assurance levels are defined, similar to TCSEC. If an organization wants ITSEC to evaluate either a product or a system, the organization identifies all the threats present in their environment. A set of security mechanisms is identified, to be introduced in the system or product, to protect them against the identified threats. Thus, the organization determines their own functional level, with the associated functional security mechanisms. The organization asks ITSEC to evaluate the system or product for a specific level of assurance, which is predefined. ITSEC will then do three things. First, it will ensure that all the functional mechanisms that were identified, are indeed integrated into the product or system. Second, that the security mechanisms are properly installed and third, it will ensure that the set of security mechanisms is adequate to protect the organization against the identified threats. In the first case the functionality is cross-checked to ensure that it is present, in the second case, assurance is given that the security mechanisms are correctly installed and can be trusted and lastly, the effectiveness is proven. The amount of rigour with which these evaluations are performed, is dictated by the assurance level that was requested for the system or product. ITSEC will thus, if successful, certify that the proposed security mechanisms introduced in the system or product are adequate to protect the organization effectively against the threats that were identified and that the security mechanisms have been tested according to a specific level of trust.

If a certificate is required to state that a specific house has a level 3 security protection, the following will have to take place:

- The threats threatening the house need to be identified, for example, theft.
- The party requesting the certificate will identify a set of safety mechanisms to protect the house against these threats, for example, door locks and a high fence.
- These identified safety mechanisms are evaluated to ensure that they are present and that they were correctly installed.

- The evaluation party will evaluate whether these security mechanisms are adequate for the identified threats, for example, will the door locks and fence be enough protection against theft.

TCSEC defined the following levels: D, C1, C2, B1, B2, B3, A1 for both functionality and assurance, as described.

ITSEC defined seven levels, E0 to E6, for assurance taking both effectiveness and correctness into account. As mentioned before, an ITSEC evaluation can be done without specifying any functional level, although ITSEC has defined levels F1 to F10 for functionality, but these levels of functionality are only used if a direct correspondence with TCSEC wants to be drawn.

It seems as if a TCSEC rating of C2 has been accepted as an industry standard for commercial environments. The following quotation from the European Computer Manufacturers Association (ECMA, 1993): ''C2 systems are the workhorses of commercial computing ... They are well-suited for the vast majority of commercial multi-user applications''. A product rated C2 will typically include security mechanisms for: discretionary access control, unique user identification and authentication, some audit control features, and more.

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 (1993) will again 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.'' This situation can be compared with the example earlier, where an attempt was made to secure a house. If a security rating of level 4 has been achieved for the house, which means door locks, burglar bars and an electronic alarm system, all approved by the SABS, and installed by a security company, were introduced, the house is not necessarily secure, because the doors may not be locked by the inhabitants and/or the alarm may not be activated. This will leave the house insecure, because the security mechanisms are not used as prescribed.

Therefore, evaluated products and systems provide a secure computing base, but are not the sole solution to secure computing environments. Similarly, a motor vehicle with all the required technical safety mechanisms, may be driven in a very reckless manner by its driver. Therefore, the driver need to be in possession of a valid drivers licence to ensure that all the technical safety features are used correctly. Technical security mechanisms need to be augmented by proper operational procedures in order to be effective.

4. Operational security

To manage, that means to introduce and maintain, a secure IT-environment, calls for a comprehensive IT security programme. One example of such a comprehensive IT security programme is GMITS, introduced jointly by the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC). ISO/IEC (1996) is in the process of developing a Technical Report, TR 13335, that will provide guidelines to an organization on how to manage a secure IT-environment. TR 13335 will eventually consist of five parts, but the first three parts address a comprehensive approach to proper IT security management, mentioned earlier.

Part 1 of GMITS, or TR 13335, is aimed at managers who are responsible for the organization's overall security programme as well as those responsible for IT security. In Part 1 the whole IT security issue is put in place for top and/or senior management. Important definitions, concepts, models, etc. are given and explained to ensure that these managers understand what is involved in IT security and that they can make informed decisions regarding IT security.

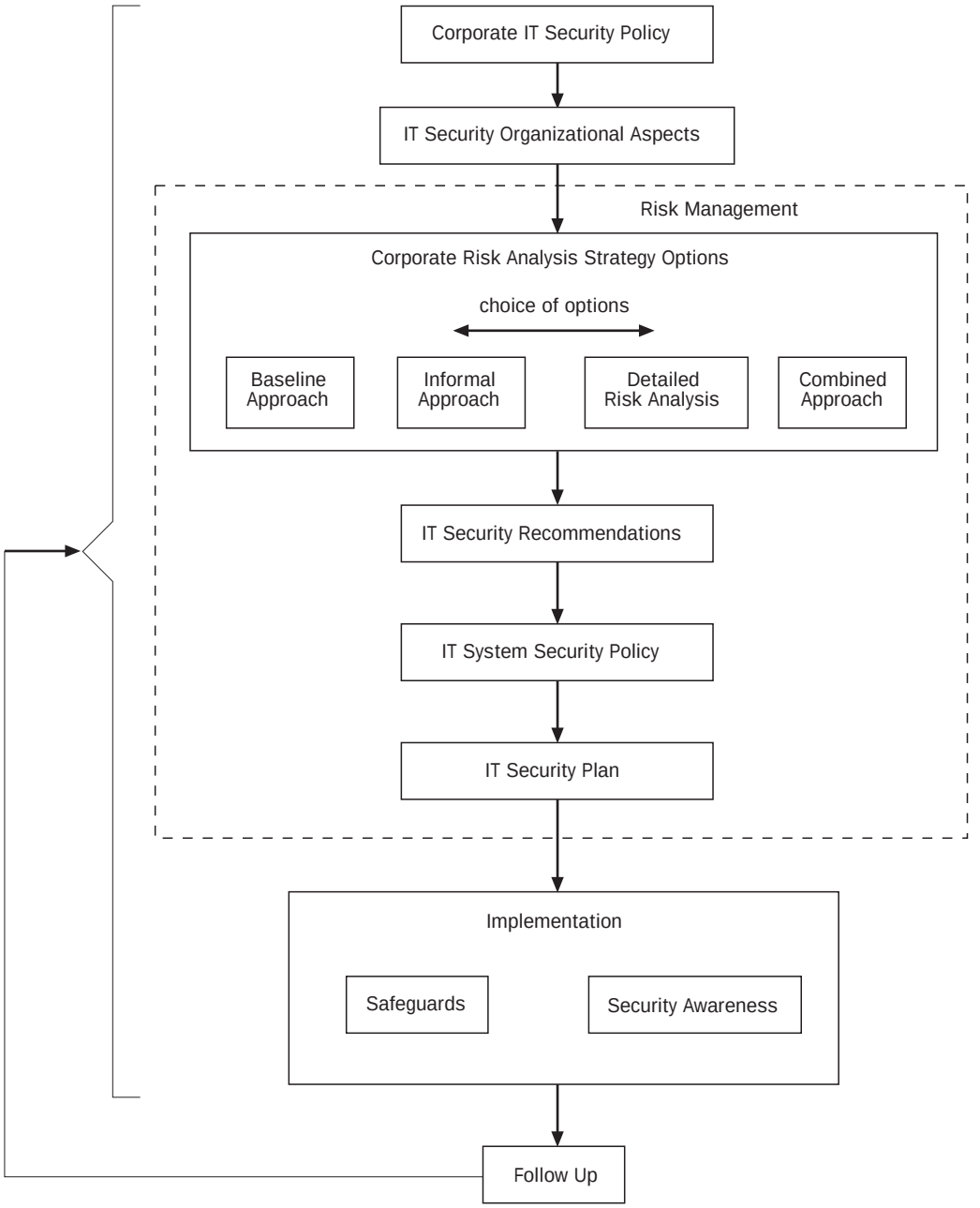
GMITS Part 2 describes IT security management and planning aspects and is relevant to, first, managers overseeing the design, implementation, testing, procurement, or operation of IT systems and second, managers who are responsible for activities that make substantial use of IT systems.

To plan and manage IT security in an organization effectively, a comprehensive IT security plan needs to be established. The following is a graphical representation of such an IT security program.

Some of these security aspects, represented in Figure 1, will be discussed briefly.

A corporate IT security policy needs to be drafted, taking the IT security objectives, strategies and other policies into account. Through such a corporate IT security policy, top management also show their commitment towards a secure IT environment.

Figure 1
The main elements in information security management



Dependent on the size and structure of an organization, every organization should define the following roles and responsibilities within their organization:

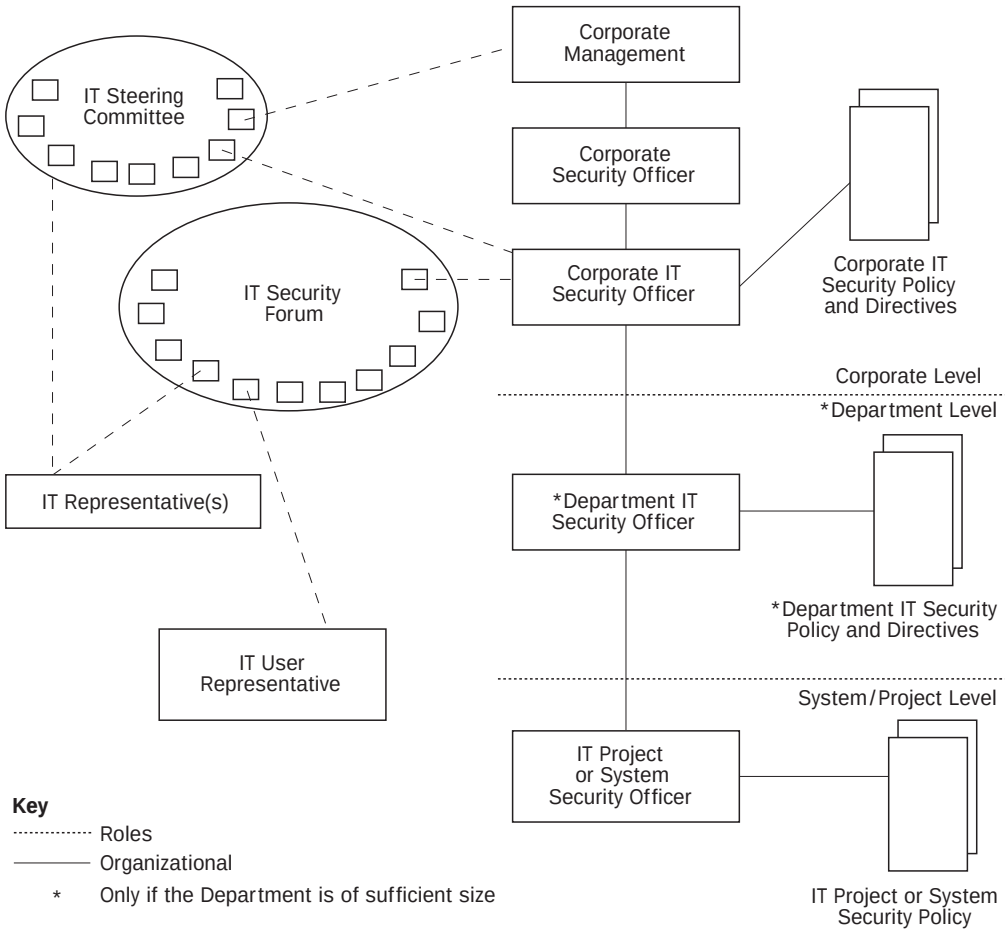
- an IT security forum, which typically resolves interdisciplinary issues and approves directives and standards; and
- the corporate IT security officer, who acts as the focus for all IT security aspects within an organization.

Figure 2 puts these IT security organizational aspects into context.

Any organization must decide on some strategy to manage the security risks specific to their environment. Basically four options are available, namely:

1 a detailed risk analysis for all IT systems in the organization;
2 an informal, pragmatic risk analysis using either internal or external security specialists;
3 the baseline approach where an organization can suggest baseline (minimum) controls to all IT systems; and

Figure 2
IT security organizational aspects



4 a combined approach where a combination of these approaches are introduced to the various IT systems.

The end result of each of these four options is a recommended set of security controls that, when successfully introduced, will reduce the extent of the security risks to an acceptable low level.

An IT security plan needs to be drafted to enable the effective implementation of the recommended controls. This security plan needs to include aspects such as: operational costs in implementing these safeguards, workloads, manpower, time schedules, etc.

Once the security plan has been drafted and accepted, the implementation of the controls takes place according to the security plan. After successful implementation of the recommended controls, it is very important that operational and administrative procedures are developed to support and enforce the technical controls.

It is very important that an effective security awareness programme should be introduced in the organization. This programme should advocate the information security policy and ensure understanding of the operational and administrative procedures and instil appropriate behaviour.

Finally, to ensure continual effective functioning of the introduced controls, it is important that the controls are maintained. Further, it is important that some security audit or compliance checking is done to ensure compliance with the IT security plan. Lastly, some incident reporting and investigation scheme needs to be put in place and preferably be integrated with the inter-organizational reporting schemes.

GMITS Part 3 describes security techniques, for example, conducting a detailed risk analysis, that can be used to implement the security concepts and elements described in parts 1 and 2. Part 3 is relevant to those parties involved with the execution of any of the security relevant aspects and elements, e.g. the information security officer.

ISO/IEC TR 13335 (GMITS) Part 1 and 2 have already been accepted as an

international Technical Report and is commercially available, but part 3 is not commercially available yet.

In conclusion, it was mentioned in the beginning that effective information security can only be obtained through an orderly, comprehensive IT security programme. GMITS parts 1, 2 and 3 may play an important role in providing such a detailed programme. Evaluated products and systems, as described previously, will play an important role in using "trusted components" in a secure IT-environment.

Introducing information security in an orderly way, using an approach like GMITS, is very important, but identifying, recommending and implementing the most effective set of security controls, technical and/or procedural, is just as important.

5. Baseline security controls

Identifying the most effective set of security controls has always been a problem. Risk analysis and management have always been recognized as the most effective approach to accomplish this. Lately, baseline security manuals are seen as an alternative technique to identify minimum security controls required by an organization. The *Code of Practice for Information Security Management* (CoP) is an example of such a manual.

The Code of Practice (CoP) has been developed by the Department of Trade and Industry in the UK, with the assistance of a group of leading international companies and organizations in the UK. The CoP was first published in September 1993 (British Standards Institute, 1993). In 1995 the Code of Practice for Information Security Management became a British standard (BS 7799). The CoP is based on a compilation of the best information security practices in general use in many leading international companies.

The objectives of the Code of Practice are twofold:

1 to provide a common basis for companies to develop, implement and measure effective security management practice; and
2 to provide confidence in inter-company trading.

From these two objectives, it can clearly be seen that the Code of Practice can be used as a common reference standard for inter-company trading and for sub-contracting or procurement of information technology (IT) services or products.

The aim of information security is to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents. One's business information, and the IT systems that support it, are very important business assets. Their availability, integrity and confidentiality may be essential to maintain the competitive edge, cash-flow, profitability, legal compliance and respected company image. Further, information security threats are expected to become more widespread, more ambitious and increasingly sophisticated. The growth of networking presents new opportunities for unauthorized access to computer systems, and the trend to distributed computing reduces the scope for central, specialist control of IT facilities. The sooner one takes action to safeguard one's information systems, the cheaper it will be for the company in the long run.

The Code of Practice consists of two parts:

1 the introduction, giving background information; and
2 the security categories and controls.

The Code of Practice is based on ten categories that should be present in most companies; these are:

1 security policy;
2 security organization;
3 assets classification and control;
4 personnel security;
5 physical and environmental security;
6 computer and network management;
7 system access control;
8 system development and maintenance;
9 business contingency planning;
10 compliance.

A comprehensive set of security controls is listed under each of these ten categories. The controls are divided into a number of logical sub-groups and each sub-group is preceded by a concise summary of the objective and scope of the group of controls.

In the Code of Practice, more than 100 controls are listed. Most of these controls are implemented by large, experienced organizations. These generally accepted controls are often referred to as baseline security controls. Collectively, these controls define an industry baseline of good security practice. Obviously not *all* controls will be applicable to every IT environment. The nature of the IT environment and the local circumstances will dictate which of these controls will be applicable in a specific environment.

A sub-set of these controls are judged to be especially important and are referred to as the key controls. The key controls will be applicable to *all* organizations, and are considered as mandatory. The key controls usually provide a good starting point for introducing information security.

These ten key controls are:

1 Information security policy document.
2 Allocation of security responsibilities.
3 Information security education and training.
4 Reporting of security incidents.
5 Virus control.
6 Business continuity planning.
7 Control of proprietary copying.
8 Safeguarding of company records.
9 Compliance with data protection legislation.
10 Compliance with security policy.

As mentioned before, the Code of Practice identified a set of baseline security controls. These controls should provide an acceptable minimum level of security to most organizations under normal circumstances. Some security risks will, however, require special treatment and protection.

The following factors are often critical to the successful implementation of information security within a company.

- Security objectives and activities must be based on business objectives and requirements, and led by business management.
- There must be visible support and commitment from top management.
- There must be a good understanding of security risks (threats and vulnerabilities) to company assets, and the level of security inside the organization.
- Security must be effectively marketed to all managers and employees.
- Comprehensive guidance on security policy and standards must be distributed to all employees and contractors.

The Code of Practice attempts to enforce these factors implicitly.

A number of countries, e.g. Holland, Australia and New Zealand, have already accepted the BS7799 as a local standard and many other countries have accepted it informally. The BS7799 is currently under revision with widespread international input. From this, it can be concluded that BS7799 may become an informal international standard or even an official international standard in the near future. Another very important factor is that the revised BS7799 will be accompanied by an evaluation and certification scheme. This may mean the beginning of an international information security ''driving licence'', who knows?

An information security certificate may become a reality sooner than many people envisage and companies without this ''driving licence'' may be left out when electronic commerce really takes off. So, get ready, prepare yourself.

6. Conclusion

Any motor vehicle on a public road requires a valid roadworthy certificate that will indicate that all technical safety and security mechanisms and features on the vehicle are present and functioning properly. The driver needs a driving licence that will indicate that he/she has learned how to drive the vehicle in a secure way by using the technical safety features correctly and effectively. Further, a third party, i.e. traffic officers, will continuously ensure that the vehicle is functioning technically well and also that the driver obeys all road usage regulations.

Similarly, an IT-environment should utilize a technically secure computer base, preferably evaluated by TCSEC or ITSEC. This computer base should be operated in a secure way and evaluated and certified as doing just that.

All of this can only be accomplished through adequate information security standards. Standards like TCSEC and ITSEC, GMITS and BS7799 can certainly provide the basis to ensure ''safe driving on the information super highway''.

References

British Standards Institute (1993), *BS 7799: Code of Practice for Information Security Management (CoP)*, PD0003, British Standards Institute, UK.

Department of Defense (DoD) (1985), *Department of Defense Trusted Computer System Evaluation Criteria (TCSEC)*, Washington, DC.

European Computer Manufacturers Association (1993), *Secure Information Processing versus the Concept of Product Evaluation*, ECMA TR/64, December.

Information Technology Security Evaluation Criteria (ITSEC) (1990), *Harmonised Criteria of France, Germany, The Netherlands and the United Kingdom*.

ISO/IEC (1996), *Guidelines to the Management of Information Technology Security*, TR 13335.