

Information Security Development Trends

E. von Solms ^a

Prof J.H.P Eloff ^b

^a Department Computer Science and Information Systems,
University of South Africa, Pretoria, SA, vsolme@unisa.ac.za

^b Department of Computer Science, Rand Afrikaans University,
Johannesburg, SA, eloff@rkw.rau.ac.za

Abstract: *Information is a very valuable resource and must be protected against harmful attacks from inside as well as outside the organization. As a resource, information is the lifeline of many organizations and is therefore vital for the survival of any organization today. Information security has developed over the last 50 years due to different development trends that have an influence on the information security environment. Information security development trends that can be clearly identified in the information security environment are best practices, certification, awareness, and the measurement of information security.*

Keywords: Information security, Information security development trends, Information security management.

1. Introduction

Information security is becoming an established discipline as more and more businesses realise its value. According to Tom Scholtz, [MET00] many organizations view information security as one of the top five issues they need to address during 2001. Many information technology (IT) organizations named information security as the number one issue after 1 January 2000. [MET00] This shows that the urgency of protecting information in organizations has become a key issue under discussion all over the world. However, unless the protection of information is correctly designed, implemented and managed, all attempts will fail.

Securing information is just as important as any other proactive action in an organization and must therefore be managed accordingly. A key aspect to the success of information security management (ISM) is the effectiveness of the management. This effectiveness can be jeopardized by different factors. Factors that have an enormous influence on information security are new technology in the business environment and security risks.

Factors such as new technology and security risks have increased the vital need for information security management in all organizations. One reason is that information security is a very dynamic action that must be effectively executed for optimum management results. This dynamic nature of information security management is due to different trends that can be found in information security.

New trends are being added to this domain each year. An information security policy is only one of many development **trends** that are important in information security management these days. The English dictionary defines a trend as: "... a course or direction of development." [ALS88]

Another trend that is very important in today's information security environment is best practices. If development trends like best practices are implemented, the results are better designs and improved implementation of information security aspects.

2. Best practices

Many organizations have a misguided sense of what it takes to address their security weaknesses. [CUT00] Many organizations are looking for a "quick-fix" tool to solve all their security problems. Cutler states that there are no "quick fixes" in information security. Organizations must treat information security as a continuous process through a set of well-managed best practices.

Best practices are the combined experiences of several companies that have already had great influence in the information security environment. Best practices are a compiled set of documents that can be used as a guideline during the implementation of different information security aspects.

According to Kisin, [KIS96] accountabilities and responsibilities must be included and clearly defined to enable best practices in an

information security management infrastructure. Many organizations develop their own guidelines based upon their individual circumstances but best practices recommend that any such guidelines should be cross-referenced to an already existing standard. [KWO97]

There are several best practices that are internationally available today for implementation in organizations. This paper will briefly investigate two of these best practices. These are the:

- British Standard for Information Security Management (BS 7799), (ISO 17799 Standard) [BRI99] and
- BSI-IT Baseline Protection Manual. [BSI98]

There are three other best practices that must be mentioned, but that will not be described in this paper. These best practices are:

- Control Objectives for Information and Related Technologies (COBIT), [COB00]
- Guidelines for the Management of Information Technology Security (GMITS)
- The Information security Forum (ISF)

2.1 BS 7799

The Draft International Standard (DIS) 17799-1 (Part 1), also known internationally as BS 7799, was created in 1995 by the British Standards Institute, with input from international multinational companies like CCTA, Shell International Petroleum Co Ltd and Midland Bank plc. [BRI99]

The origin of BS 7799 goes back to the days of the UK Department of Trade and Industry (DIT) and the Commercial Computer Security Centre (CCSC). BS 7799 was first issued in 1995 to provide a comprehensive set of controls comprising best practices in information security. It is intended to serve as a single reference point for identifying the range of controls needed for most situations. [BRI99]

BS 7799 is comprehensive in its coverage of security issues. It contains a substantial

number of control requirements, some extremely complex. These security controls contain further detailed controls, bringing the overall number somewhere in the region of more than 500 controls and elements.

According to Mr Wills, [CCU99], Minister of Small Firms, Trade and Industry of Britain, BS 7799 is an excellent example of an industry-developed standard that is now being adopted by the public sector. ISO/IEC 17799 aims to allow compliant companies to publicly demonstrate that they can safeguard the confidentiality, integrity and availability of their customers' information. [GAM99]. Part 1 contains more than 100 controls to measure information security.

2.1.1 Composition of BS 7799

Part 1 of BS 7799 (ISO/IEC 17799) defines about 127 security controls structured under ten major headings to enable readers to identify the particular safeguards that are appropriate to their particular business or specific area of responsibility. The ten headings are listed below. [BRI99]

Section 1: Security policy

Section 2: Security organization

Section 3: Assets classification and control

Section 4: Personnel security

Section 5: Physical and environmental security

Section 6: Communications and operations management

Section 7: Access control

Section 8: System development and maintenance

Section 9: Business continuity management

Section 10: Compliance

BS 7799 provides a well-proven framework of best practices to implement, maintain and document information security within the organization. [CCU99] From what has been investigated above, the author states that BS 7799 is one of the leading international best practices that can be implemented in an organization in order to prevent security risks.

2.2 BSI-IT Baseline Protection Manual

BSI-IT Baseline Protection Manual [BSI98] is a best practice that provides recommended measures for meeting medium level protection requirements in an organization. The 1998 version of this document has been revised and the newer BSI version has been available since 2000 [BSI00]. Some extra information is included and some changes have been made to the 1998 version. But overall, the two versions are almost the same. In the rest of this paragraph, the 2000 and 1998 versions will be used as references.

The BSI-IT Baseline Protection Manual addresses aspects like stand-alone systems, networks/servers, telecommunications, and infrastructure and information security management. The last aspect, information security management includes information security processes, from the planning stage to the maintenance of information security. The five processes that are addressed in information security management in the 1998 version include [BSI98]:

- Development of an IT security policy
- Compiling IT security concepts
- Implementing of the IT safeguards
- Training
- IT security during current operations

The BSI documentation [BSI98] states that in the modern world of information is increasingly supported by the use of information technology (IT). Numerous work processes are electronically controlled and large amounts of information are stored as digital data, processed electronically and then transferred through local and public networks.

Some public or commercial tasks are not possible without IT, others only partially. As a result, many institutions in both administration and industry depend on the perfect operation of IT. It is only possible for authorities and companies to reach their goals if IT systems function correctly and reliably. [BSI98]

The 2000 version depicts the processes as follows: [BSI00]

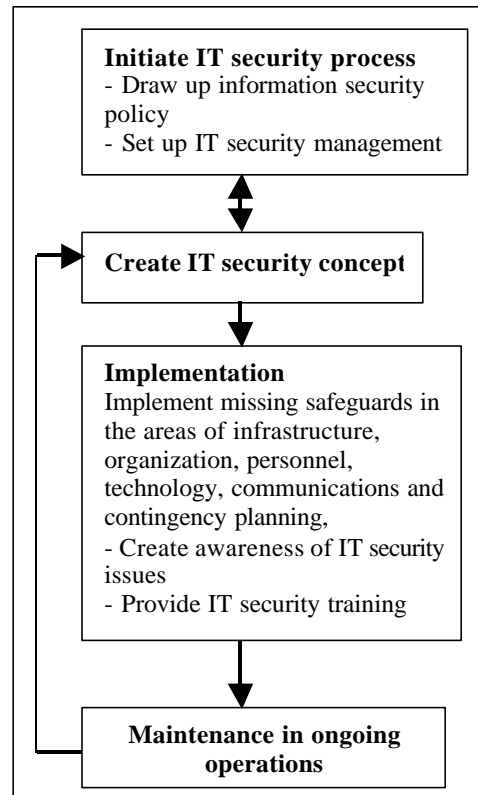


Figure 1: IT security process

BSI documentation states that IT security is to be seen as an integral part of the primary task. As a result, the responsibility for the secure and correct fulfilment of IT tasks must be delegated in the same way as the responsibility for the primary task itself. As is the case with the primary task, the ultimate responsibility for IT security rests with management. The corporate tasks required for IT security, the organisation, delegation of responsibilities and the necessary controls, are co-ordinated by a specially established organisational unit, the security management team.

3. Certification

The complexity of today's information security environment makes it very difficult to assess information security in any given organization. This can be a big problem because the assessment of information security is vital for trust in any organization. According to Andersen, [AND97] a reason for this is that certain information security measures will only be trusted if users have confidence that they are using systems which have been certified by public entities.

Two methods that are widely available for assessing business products and services today are evaluation and certification. There is a big difference between evaluation and certification in the business world. The definition of evaluation is that a particular software or hardware product must meet specific requirements. There are a number of different evaluation criteria available today for evaluating information products. These are, for example, the Common Criteria (CC) and Information Technology Security Evaluation Criteria (ITSEC).

The definition of certification is to establish if a process or service meets the given (minimum) requirements. According to Von Solms, [VON01] certification is an acceptable way to assess the level of information security in a company. He also states that the results of the certification can then be compared to certification results from other organizations. Although certification has only been around for a few years, a lot of groundwork has already been done about certification as an information security development trend. [RAN00][VAN97][ELO00b]

Certification schemes provide a reputable means for organizations to measure their information security management against best practices. These help businesses to safeguard their vital information assets. Secondly, it allows businesses to demonstrate that they comply with a specific information security standard. There are only a few certification schemes available in today's information security environment. These schemes include:

- C:cure
- ISIZA
- BSI – certification scheme

3.1 C:cure

Lack of confidence between trading partners can be a major barrier to electronic commerce. In order to provide organizations with an independent means to demonstrate to trading partners and customers that they comply with BS 7799, the c:cure (pronounced 'secure') certification scheme was developed. [BRO00]

The c:cure certification scheme for accredited certification was launched in 1998 by Mrs. Barbara Roche, UK Minister for Trade and Industry. As a means of allaying fears about information security, the scheme was developed for the Department of Trade and

Industry (DTI) by BSI-DISC, with the help of the United Kingdom Accreditation Service (UKAS) and in close liaison with industry representatives. [CCU99]

The c:cure scheme is entirely voluntary – there is no obligation by law or regulation that any organization must undergo certification. The scheme enables organizations of all sizes and in all sectors to gain BS 7799 certification, proving that they have adopted sensible, appropriate security measures to protect their own and their trading partners' information. [BRO00] C:cure is designed to cover all sizes and types of organizations, down to the smallest firm and it can even cover bits of organizations, such as particular divisions or trading sites.

Nordin [LEI00] points out that the BS 7799 information security management certificate (c:cure) may be of most interest to business partners who entrust information to the certificated organization. It will also affect the management of the company itself, which must demonstrate adherence to good security practices. C:cure is a certification scheme that can be used accredited third-party certification. Accredited third party certification (certification body) offers a competent and unbiased view of the security properties of an organization's systems.

C:cure uses independent certified auditors from certification bodies with demonstrable competence in the key areas of IT and information security management. The auditors judge the information security management controls against a risk assessment of the threat faced by the organization. The independent UK Accreditation Service, in turn, accredits the certification bodies. [CCU99]

The c:cure World Report [CCU99] states that c:cure is designed to cover all sizes and types of organizations, down to the smallest firm. It can do this because it uses risk assessment based on unique threats faced by the organization being tested. C:cure is aimed at providing a level of confidence for organizations and their trading partners regarding the security of their IT assets. [ELO00]

3.1.1 Review of c:cure

The c:cure Steering Committee met on 2 October 2000 to continue their review of the viability of the c:cure Certification Scheme. The meeting recommended that the c:cure

scheme should be discontinued in favor of alternative BS 7799 certification. The reason for a possible discontinuing of c:cure is the following. The c:cure certification scheme has the stand point: “all or nothing”, so, there are no incremental approach to c:cure. To prepare a company for the full certification of c:cure takes a long time and a great deal of effort. All the problems mentioned above lead to a low take up of the c:cure certification scheme.

According to Von Solms, [VON00c] the problems with BS 7799 certification (all or nothing) have been identified by specialists in South Africa and an adapted approach had been developed. This resulted in the recent establishment of the Information Security Institute of Southern Africa (ISIZA). The next paragraph gives a brief overview of ISIZA, the newest approach to certification.

3.2 ISIZA

ISIZA, the acronym for the Information Security Institute of South Africa, was launched in the early months of 2001. ISIZA is an information security authority that was designed for South Africa. Its aim is to address the lack of information security framework to protect industry stakeholders.

According to Opperman (head of ISIZA), [SAI00] an increasing number of South African companies are beginning to embrace e-business practices. He goes on to state that certification of these companies' information security systems will become an essential prerequisite in order to exchange information globally.

ISIZA will create an Advice Committee consisting of corporate companies within the industry. The Advisory Committee will create the different levels (5) based on ISO BS 7799. [VON00c] These levels mean that the ISIZA model is based on incremental certification. That means were BS 7799 has an “all or nothing” approach, ISIZA will have different levels of certification.

The first level is an introductory level and consists of a selection of BS 7799 controls. Level 2 follows on level 1 and includes more BS 7799 controls. At the moment, only level one is totally finalize, while level 2 is still being defined. In the near future, ISIZA's levels 3 and 4, with level 5 (being the full BS 7799 certification), will also be implemented. [VON01]

Von Solms [VON01] also states that a company can get an initial ISIZA certificate must faster, by conforming to a small subset of BS 7799 controls that will make up level 1. He goes on to state that the companies can move incrementally to higher levels overtime, until the full BS 7799 certification level is eventually reached.

It is the whole idea of the different levels that makes ISIZA unique. That means that if an organization wants to be BS 7799 certified, the organization can decide for themselves what specific certification level (level 1 to 5) they require. The organization can then upgrade (on their own time) the level and pace, and eventually reach full BS 7799 certification.

3.3 BSI – Certification scheme

The 2000 version of BSI [BSI00] addresses information security certification. As the IT-Baseline Protection Manual (with its recommendations as to standard security safeguards) has come to assume the role of an IT security standard, it is fitting that it should be used as a generally recognised set of criteria for IT security.

In future it will be possible for an institution to obtain the IT-Baseline Protection Certificate for a selected set of IT assets when an independent, accredited body can demonstrate from a basic security check that the required IT baseline protection standards relating to security safeguards have been implemented. [BSI00] At the moment this certification scheme is not available for implantation and use.

4. Information security policy

A development trend that influences information security management is the enforcement of the information security policy. Before organizations can start to manage information security, they must have an information security policy in place that will be used as a guideline to **how and what** must be managed.

An information security policy may be defined as: “compiled documentation of computer security decisions.” [NIS00] These security decisions can be made with regard to hardware, software, networks and information. One purpose of an information security policy is to protect the organization's information assets from all threats, whether internal or

external. All organizations must have an information security policy in place. This is to make sure that all information is correctly and fully secured.

Lewis [LEW00] states that the presence of a formal information security policy is one of the most important issues in reporting and resolving security breaches. The assumption is, then, that an information security policy is no longer a luxury but a total necessity for any organization wanting to secure its information.

Many documents have already been published about the importance of an information security policy in the organization. Although there is much information available on this topic, there are still many organizations that do not adhere to it. In a survey held by ISBS 2000, [DEP00] only 58% of the organizations interviewed considered information security to be an important business issue; only one in seven has a formally defined policy describing their information security management system.

The information security policy trend has undergone a huge shift in focus over the last couple of years. A few years ago many organizations had a properly designed information security policy, but were not implemented. The information security policy was probably stored somewhere on a shelf instead of being used and managed. When information security management began to gain prominence, it was accompanied by a lot of controversy surrounding the failure to manage the information security policy. Critics were stating that if an organization did not manage its information security policy, this was just as bad as not having an information security policy at all.

An aspect that must be remembered when implementing an information security policy is that it is vital to ensure that the information security policy has the commitment of senior management. Only if senior management takes responsibility for the information security policy, can the organization force employees to do the same.

5. Information security awareness: A human issue

Information security awareness is a widely publicized and talked about issue in the business environment. The reason for this is that information security awareness is mainly a human-related issue. It is important to realize

that “human issues” are the main cause of security breaches. [LEW00] The only way to reduce information security risks in an organization is to make employees more information security aware. This awareness also means that employees must take responsibility for their own actions in the workplace.

The information security awareness development trend started in about 1980 where the responsibility of information security was the job of one specific person. The rest of the employees had little or no knowledge of information security. In the early 1990s the idea that all employees must understand and implement information security come to the foreground. The reason for this was that more employees started to work with sensitive information.

Organizations also realized that before they could enforce employee responsibility, they had to ensure that all employees understood information security issues. Employees cannot be held responsible for their actions if they are not aware that information security exists and how their actions can directly or indirectly influence information security. One way to present information security to employees is by means of an information security awareness programme. This information security awareness programme can be used to ensure that the security policy and best practices are implemented and complied with.

6. Continuous measurement of information security

An organization may have implemented an information security policy but still have security problems. The reason is not that the information security policy is badly or poorly written, but rather that nobody knows whether the policy has been enforced or not. This happens because there are no mechanisms in place, apart from some annual audits, to ensure that they are enforced and complied with on a continuous basis. According to Kisin, [KIS96] regular monitoring for compliance must be practiced if information security policy and other standards are to be taken seriously by employees.

Internal audits are done once a year to have a closer look at whether the information security in the organization is working as it should and that the security policy is being enforced. The problem that develops is that, during the rest of

the year, the company is open to security attacks because no one is checking for security problems outside this audit period. The solution to this problem is to start measuring and monitoring information security in an organization on a continuous basis. Only by measuring and monitoring information security, can an organization find out if the information security policy and best practices are being enforced

7. Conclusion

This paper has discussed different development trends that can be found in an information security environment. The first development trend that was mentioned was best practices. Best practices only became part of the information security environment in the last few years. However, best practices already have a big influence in how organizations view information security.

Another development trend that is becoming more important in information security is certification. This paper gave a brief overview of different certification schemes. The remaining development trends mentioned in this paper were information security policies, awareness, and measurement of information security.

There are some other development trends not mentioned in this paper, these include information security ethics, legal aspect and senior management.

8. References

- [ALS88] Alswang J. & Van Rensburg A. 1998: "An English usage dictionary." Edducum Publishers, Cape Town.
- [AND97] Anderson M. 1997: "The role of Government in creating the IS security infrastructure." Proceedings of IFIP TC11, 13th international conference on Information Security.
- [BRI99] British standard 7799 Code of Practice 1999: "Information security Management – Part 1: Code of Practice for information security management." Online: <http://www.c-cure.org/fbs7799.htm>
- [BRI00] Briney A., 2000: "Security Focused." Online: http://www.infosecuritymag.com/articles/september00/pdfs/Survey1_9_00.pdf
- [BSI98] Budensamt fur Sicherheit in der Infromationstechnik (BSI). 1998
- [BSI00] Budensamt fur Sicherheit in der Infromationstechnik (BSI). 2000. Online: <http://www.bsi.bund.de/>
- [CCU99] c-cure World, Online: <http://www.c-cure.org>
- [COB00] COBIT Steering Committee, 1998: "COBIT" 2^d edition. Information Systems Audit and Control Foundation.
- [CUT00] Cutler K., 2000: "Hitting the bull's eye." Online http://www.infosecuritymag.com/articles/august00/columns5_logoff.shtml
- [DEP00] Department of trade and industry, 2000: "Information Security Management Policy." Online: <http://www.dti.gov.uk>
- [ELO00b] Eloff M.M. & Von Solms S.H., 2000: "Information Security Management: An Approach to Combine Process Certification and Product Evaluation." Computer& Security, Vol 19 No 8.
- [GAM99] GAMMA: "BS7799" 1999", Online: <http://www.gammasl.co.uk/topics/hot1.html>
- [GMI00] Guidelines for Management of IT Security – GMITS, Online: <http://www.cancert.ca/Pages/ISSStandards.htm#Guidelines>
- [KIS96] Kisin R. 1996: "IT Security – Implementing 'best practices'." Computer Audit Update, January 1996, Elsevier Science Ltd.
- [LEI00] Leirgulen S.I., 2000: "Protect your most important asset." Online: <http://www.dnv.com/>

- [LEW00] Lewis A. 2000: "*Time to elevate IT Security to the boardroom.*" E-Secure, August 2000, Vol 1, Issue 1.
- [MET00] Meta Group 2000: "*Service Management Strategies.*" Online: www.metagroup.com
- [NIS00] NIST: National Institute of Standards and Technology. "*An introduction to Computer Security*", The NIST Handbook." Also available online: www.nist.gov/
- [RAN00] Rannenber K., 2000: "IT Security Certification and Criteria." Proceedings of IFIP TC11, 16th international conference on Information Security.
- [VON97] Von Solms R. 1997: "*Can Security Baselines replace Risk Analysis.*" Proceedings of IFIP TC11, 13th international conference on Information Security.
- [VON00c] Von Solms S.H., 2000: "*Information security- The third wave*" Presented at Best Synergy Conference, October 2000.
- [VON01] Von Solms SH.,2001: "*Certification of your company's information security level.*" Secure IT , February 2001.