

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Implementing an Information Security Management System (ISMS) Training process

G7799

Practical Assignment

Version 1.1

Craig S Wright

BDO Chartered Accountants

SANS Darling Harbour
2005

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

Abstract 1
Document Conventions 2
1. System Definition 3
Introduction 3
Scope of the ISMS 3
Goals of the ISMS 4
The Organisation 5
Organisational roles and responsibilities 5
Organisation Head and Directors 5
Chief Information Officer (CIO) 6
Information Security Manager 6
Departmental Managers 6
Other Staff and Information Users 7
2. Plan, "establish the ISMS" 8
Training Project Implementation Plan 9
1 Scope, Goals, and Objectives 10
2 Resources 10
3 Target audiences 11
4 Motivation 11
5 Development and implementation of the programme 12
6 Regular maintenance 14
7 Periodic evaluations 14
Policy, Standards and Guidelines 15
Awareness 15
Training 16
Education and Professional Development 16
Corporate Policy and Standards for Awareness and Training 16
Risk Management 18
Primary Risks and Controls 21
Information Assets 27
3. Do, "Implement and operate the ISMS" 28
Problems, Actions and Steps 28
Awareness Programmes need to be implemented 29
Training Programmes need to be developed 33
Cost Considerations 34
Statements of Applicability 34
4. Check, "monitor and review the ISMS" 36
Training AudIT and Checklists 36
System Improvement Monitoring and Checks 41

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

5. Act, “maintain and improve the ISMS” 44
System Maintenance 45
Where Next? 46
Conclusion 47
Appendixes 48
Appendix A, Detailed trainer guide for conducting the awareness workshops 48
Introduction 48
Definition of Workshop 48
The Workshop Outline 49
Guidelines for use of tools 49
Conclusion 49
Appendix B, Example slide content 51
Introduction - Slide 1 51
What are the issues - slide 2 52
What is information - slide 3 53
What is information security - slides 4 - 6 54
Threats - slide 7 55
Threats – slide 7 - 9 55
Threats – slides 10 – 14 57
Threats - slide 15 57
Threats - slide 16 58
Motives - slide 17 58
Targets - slide 18 - 19 59
Information security documentation - slide 20 59
Your role in information security - slides 21 - 30 61
The 10 Commandments of IT Security – Slides 31 - 32 69
The future of security – Slide - 33 70
Summary –Slide 34 71
Where to get more information – No slide at present – 35 71
Appendix C, Sample Managerial assessment interview questionnaire 72
Computer Security Awareness – Example Quiz copied from the Fermi National Accelerator Laboratory 73
Computer Security Awareness checklist: 73
Example - Security Awareness Evaluation Form 75
Appendix D, Sample awareness materials 77
Appendix E, awareness and training metrics 82
Sample Human Resources Checklists 82
Appendix F, Training Programme Planning Template 84
As modified from NIST Special Publication 800-50 84
Executive Summary 84
Background 84
Relevant IT security policy 84
Awareness 84
Training/Education 84
Professional certification 86

© SANS Institute 2000 - 2005 Author retains full rights.

Resource requirements and funding 86
Bibliography 87
Organisational References 87
Published References 89
Web Sites 90

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

List of Figures

Figure 1 - Plan Do Check Act (PDCA) process 3
Figure 2 - The Training Summit 9
Figure 3 - AS/NZS 4360 - Risk Management Overview 19
Figure 4 - Sample awareness materials 1 77
Figure 5 - Sample awareness materials 2 78
Figure 6 - Sample awareness materials 3 79
Figure 7 - Sample awareness materials 4 80
Figure 8 - Sample awareness materials 5 81

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Abstract

One of the key controls within any ISMS[1] is it the continued awareness and training of staff and other parties. The focus and topic of this paper consists of the development of an ISO-17799 compliant training system. The purpose of this paper is for submission as a practical assignment towards SANS G7799 certification.

Training is an essential part of any ISMS. The development and maintenance of suitable training systems is critical to the success of any organisation's overall ISMS.

This paper will develop an ISMS concentrated on the training requirements of an organisation. The document covers all aspects of the ISO-17799 guidelines and the PDCA process. A definition of the requirements, planning and risks associated with the development of a training programme suitable to ensure that adequate training is deployed within an organisation will be covered. This paper will also cover the basics of developing information security awareness, training and education programmes as well as the processes involved in the maintenance of the programme.

Some of the areas covered within this paper include the design of awareness and training programmes, the development of training materials, the implementation of the training programme (including delivery) and post implementation feedback.

This paper shows the development of a training regime fully compliant with the “plan, do, check, act” process across the life cycle of the security awareness and training programmes.

[1] ISMS – Information Security Management System

© SANS Institute 2000 - 2005 Author retains full rights.

Document Conventions

When you read this practical assignment, you will see the representation of certain words in different fonts and typefaces. The representation of these types of words in this manner includes the following:

`command`	The representation of operating system commands uses this font style. This style indicates a command entered at a command prompt or shell.
`filename`	The representation of filenames, paths, and directory names use this style.
`computer output`	The results of a command and other computer output are in this style
URL	Web URL's are shown in this style.
Quotation	A citation or quotation from a book or web site is in this style.

© SANS Institute 2000 - 2005

© SANS Institute 2000 - 2005 Author retains full rights.

1. System Definition

Introduction

Effective awareness and training schemes are essential to the continued defence of an organisation's security. This paper details the development of an Information Security Management System (ISMS) designed to fulfil the training requirements of an organisation compliant with the ISO 17799 standards.

This document details the stages in developing an ISMS based training regime that is compliant with Plan Do Check Act (PDCA) process.

Scope of the ISMS

The scope of this paper details all of the stages required in the planning, improvement, execution and continuation of an ISMS training regime.

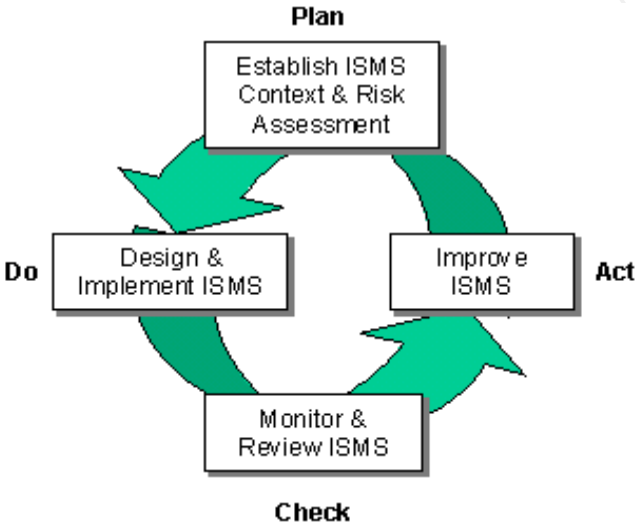


Figure 1 - Plan Do Check Act (PDCA) process

Training requirements for the implementation of ISO 17799 within an organisation include development of an information security awareness programme as well as training and education programmes. The scope of this document encompasses all staff within the organisation with access to IT information assets. This ranges from employees up to executive management and all levels in between.

This document does not end at awareness training alone, but includes the necessary education and training requirements of staff within the organisation. The continuing development of individuals within the organisation, their education within their roles (especially within IT itself) and the topic of certification are all within the scope of this paper.

The continued success of the organisation's overall information security process depends on all members of an organisation and requires that all members understand the security requirements.

© SANS Institute 2000 - 2005 Author retains full rights.

Goals of the ISMS

The primary goal of the ISMS is to ensure that all personnel involved with the use and management of the organisation's information assets have an understanding of the information security policy, standards, procedures and other requirements to an acceptable level.

This document has been developed in order to facilitate the creation and maintenance of a comprehensive information security awareness programme, and an information training and education programme.

People and not technology are generally the weakest link in information security control. Awareness and education is essential in developing a "human firewall"[2] and the associated mental processes that this entails. In his essay, “The Human Firewall”, Christopher details the exposure organisations face from the human factor.

Some of the critical success factors effecting the development of a training awareness programme include:

- Developing an understanding of the business drivers and strategies within the organisation,
- Identifying the key threats and perils related to these activities,
- Understanding the nature and priority of the organisation’s security requirements
- Analysing the security implications of the network topology
- Analysing the key security components of the network design
- Analysing the security characteristics of key applications related to external connections and business activities
- Understanding the security implications of future business plans and the impact that they may have on the current network topology and components.
- The costs of the awareness programme need to be commensurate with the benefit it delivers,

[2] “The human firewall”, Christopher, Abby, 28/10/2003

© SANS Institute 2000 - 2005 Author retains full rights.

- In addition, the cost of a training programme must be measured against IT benefit to the organisation. Is important to consider the cost of external resources, versus internal training,
- The awareness and training programmes must be delivered at the level of the audience. It is crucial to ensure that these sessions are delivered at a level that is designed to maximise understanding for the audience.

All of the afore-mentioned points must be taken into consideration when developing the ISMS.

The Organisation

This ISMS is primarily developed for a state government owned corporation involved in the implementation of an ISMS compliant to the AS/NZ 17799.2 standards.

The organisation is currently undertaking a restructuring, where it is merging several related organisations into one large organisation. For this reason, information security awareness training and general education are critical factors to the continued security of the organisations infrastructure and information.

The current transitional nature of the organisation's structure and policies makes the timely development of an ISMS even more critical. This organisation's role and place within Australia's critical infrastructure makes it especially important that an information security training and education programme is developed correctly. It is just as critical that this process is maintained adequately in a manner that continues to support the organisation.

This ISMS could be easily redeveloped for deployment within other organisations. There is a universal need for awareness and training in all organisations regardless of size and focus.

Organisational roles and responsibilities

The chain of responsibility for information security awareness, training and education essentially needs to be understood across the organisation. The organisation's information security programme has not reached maturity and is still developing. At this early stage, it is crucial all members within key positions in the organisation understand their respective responsibilities.

Organisation Head and Directors

© SANS Institute 2000 - 2005 Author retains full rights.

The head of the organisation and the directors need to ensure that sufficient priority and resources have been allotted to the information security awareness, training and education processes. A CIO has been appointed and responsibility has been assigned within the organisation.

Chief Information Officer (CIO)

The responsibility to administer training and security awareness lies with the CIO. It is the CIO's responsibility to ensure that an overall strategy for information security awareness, training and education is in place.

This is a responsibility to ensure that:

- The programme is adequately funded and resourced,
- That feedback and other controls or reporting are in place,
- That the programme is implemented effectively.

Information Security Manager

When considering information security, it must be remembered that this is not all online. The organisations information that exists in multiple formats, and as such, both physical and electronic security need to be taken into account when developing programmes for awareness and training.

The Information security manager is responsible for the development of training materials, and their effective deployment. The information security manager needs to ensure that all training materials for information security are developed in an appropriate manner and that they are delivered to the intended audiences in the most effective manner.

The information security manager must ensure that awareness training and education for information security within the organisation is constantly reviewed and updated to maintain IT relevance to the organisation.

The information security manager needs to liaise with other management within the organisation, such that they may provide critical responses and other feedback on the material, the presentation and the level of awareness and training within the organisation.

Departmental Managers

Departmental managers are generally, the owners of the information within the organisation. As such, it is their responsibility to ensure the relevance and acceptance of the policies, standards and procedures concerning security as it pertains to their department.

Information security is not just a function of IT As such departmental managers

© SANS Institute 2000 - 2005 Author retains full rights.

need to understand that they are responsible for ensuring that their staff are aware, and comply with the information security awareness and training requirements of the organisation.

Departmental managers will often serve in the role of the data owner. Departmental managers should act as a "Policy Evangelist" or "Policy Entrepreneur"[3] within the organisation continually pushing the need for adequate awareness and training of staff in IT polices and procedures. Kindon's (1984, p.129) "Public policy entrepreneurs" provides us with a contextual model within the organisation.

Other Staff and Information Users

Information users within the organisation include:

- Full and part-time employees,
- Contract staff,
- Personnel from government departments and associated organisations,
- Employees of various outsourcing firms.

General users need to ensure that they work with management to meet their training and education needs in a manner relevant to the organisation. It is the user's responsibility to comply with the organisation's information security policy, procedures and standards.

[3] Kindon, John W. (1984), "Agendas, Alternatives and Public Polices", Boston, Little, Brown.

© SANS Institute 2000 - 2005 Author retains full rights.

2. Plan, "establish the ISMS"

The a success of a security programme, as defined in the NIST[4] documentation consists of the following stages;

1. developing IT policy that reflects business needs tempered by known risks;
2. informing users on the key security responsibilities, as documented in the security policy and procedures; and
3. Establishing processes for monitoring and reviewing the programme.

It is crucial that the senior management and executives of an organisation lead by example. All users within the organisation must be aware of the need for security and of their responsibilities in order that for any security programme to be successful.

It is crucial to understand that awareness is not training or education. Rather, awareness is the first stage in developing a culture of security within the organisation. Security awareness allows people to understand their role within the organisation from an information security perspective. Awareness helps people realise the need for further training and education.

In planning the development of awareness, training and education programmes it is essential to first understand the each of these are a separate stage that builds upon the next. Initially security awareness sessions help users improve their behaviour from an information security perspective. Awareness sessions allow users to become knowledgeable in their responsibilities as they are taught correct practice within the organisation. Development of awareness across all users helps improve accountability, one of the key tenements of creating a secure environment.

It is important that employees are trained to understand their roles and responsibilities from an information security perspective in order to show that a standard of due care in protecting the organisation's information security assets has been implemented.

No staff member may be expected to conform to the organisation's policies standards and procedures until they have been informed adequately. As a result, these users pose a risk to the security of the information assets belonging to the organisation.

[4] NIST (National Institute of Standards and Technology) Special Publication 800-50

© SANS Institute 2000 - 2005 Author retains full rights.

Security awareness programmes help users understand their responsibilities, and allow the users to address the need for a security within their role.



Figure 2 - The Training Summit

Awareness starts as the first stage of an information security awareness, training, and education programme. It by no means ends at this stage. Awareness is a continuing process that should be used to reinforce the training and education stages of the programme. Awareness is a continuing process to alter the user's behaviour and attitudes.

Training Project Implementation Plan

For any information security awareness and training programme to be successful, detailed planning is essential. The planning of awareness and training programmes must consider the whole life cycle from the beginning of the process to completion. The following seven steps as developed in the NIST CSAT[5] programme may serve as a starting pointing the development of the programme:

1. the programmes Scope, Goals, and Objectives need to be identified;
2. the programme trainers need to be selected;
3. target audiences within the organisation need to be selected;

[5] NIST Computer Security Awareness and Training (CSAT)
An Introduction to Computer Security: The NIST Handbook (Special Publication 800-12)

© SANS Institute 2000 - 2005 Author retains full rights.

4. motivational goals for all members of the organisation are defined;
5. the programme is implemented;
6. A routine of regular maintenance will keep a programme up to date
7. Periodic evaluations need to be done on the programme to maintain IT relevance.

1 Scope, Goals, and Objectives

The first stage of developing an awareness-training workshop requires an understanding of the challenges faced by the organisation. An awareness of the risk issues facing an organisation is essential to develop action plans to address the challenges that they face.

Goals are set for all stages of the programme. There should be goals for security awareness, security training, education, and maybe even certification within the organisation.

One of the organisational goals and an associated government requirement is to achieve AS/NZS 17799.2-2003 certification. ISO 17799 has a mandatory requirement for periodic training in information security awareness. The scope and goals of this programme, and thus the objectives need to take into account this mandate.

The goal of this programme is to “raise the bar” of awareness and knowledge of information security concerns across the entire organisation.

The primary objective of this programme is to create and then maintain an appropriate level of protection for all the information resources within the organisation by the dissemination of information to all corners of the organisation. It is crucial that the awareness of information security processes, controls and responsibilities be improved and constantly maintained.

Individual objectives need to be set on a business unit and a part mental level as well.

2 Resources

It is essential that the stakeholders in the development of an ISMS awareness-training regime should include key representatives of the organisation for business management, network architecture and management, platform management, information security management and application development and support.

Additionally, training staff need to be selected. Whether internal employees are used or contract services are sourced, it is important to ensure that the trainers

© SANS Institute 2000 - 2005 Author retains full rights.

are well versed in information security techniques and principles and have detailed knowledge of the organisation's policies, procedures and standards.

It is important to remember that all awareness and training processes are implemented in order to satisfy business needs of the organisation. Any programme that does not consider the costs and availability of resources will not succeed.

The creation of an awareness programme involves more than just training. Resources need to be allocated (either within the organisation or sourced externally) to create and maintain the awareness process. A good example of this is the need to constantly cycle posters used to remind employees of their responsibilities. If these are not regularly changed, the employees will quickly start to ignore them as they fade into the background.

The ISMS Committees

As a part of the ISMS management group, a training subcommittee will be formed. The subcommittee will report to the ISMS steering committee. The ISMS training subcommittee will have representation from the management groups in the relevant departments, the training department, the information security officer and the risk management group.

3 Target audiences

When assessing the needs of the organisation, it is important to remember that not all users have the same requirements. Whereas security awareness is a key requirement for all users of the organisation, advanced training and even certification may be not only be unnecessary to the organisation when applied to all users, but may be detrimental.

Awareness programmes should be segmented, based on the level of awareness and knowledge of the users to the organisation's security requirements.

Training and education programmes are best segmented based on the role of the individual within the organisation. The users may be segmented into groups such as users, system administrators, management or other relevant organisational demographics.

Further training segmentation may be required based on the individual users job category or level of existing computer (and in particular, information security) knowledge.

4 Motivation

As programme evangelists, key management need to understand how these

© SANS Institute 2000 - 2005 Author retains full rights.

programmes will benefit the organisation. Motivating management and executives relies on creating awareness of the need for information security training programmes and the risks associated with not implementing these programmes adequately.

To further motivate the employees within the organisation and to ensure that management not only accept but embrace the programme, a series of ”carrot and stick” processes need to be implemented. Key to this is the linking of security processes to employees KPI’s. Additionally, management need to have their bonuses linked to the performance of their staff in respect of the organisation’s security. HR needs to implement disciplinary processes for breaches of the security process and standards within the organisation.

By alerting management to the risks faced by the organisation and the possible losses that may be reduced through the implementation of these programmes, they are more likely to evangelise the programme. Management buy in to the programme is the only way to obtain the necessary resources. For this reason, by in is important across all levels of management within the organisation.

Individual employees of the organisation cannot be expected to comprehend the value of the information assets they use in respective roles without adequate training. By involving individual employees in the development of this programme actively, they are likely to be both more aware of the requirements for information security and more likely to support the programme.

5 Development and implementation of the programme

Covered further in the DO stage, development involves the creation of the programme.

Research needs to be done continuously in order to determine the training needs of the organisation. Users must be made aware of –

- The continuing importance of security to the organisation,
- The fact that they are accountable for their actions, and
- The possible consequences that may occur from a breach of the policies, standards or procedures of the organisation.

All users need to be aware that information security directly relates to their terms of employment.

Management should devise an action plan for addressing near and long-term issues as well as formulating a strategy to ensure that all parties are aware of it.

It is important that the security awareness and training programmes are highly visible within the organisation and the training methods are selected and presented based on the needs of the individual organisational demographics

© SANS Institute 2000 - 2005 Author retains full rights.

needs.

Cooper et al's dissertation[6] shows that the design considerations used for the development of the awareness and training programmes must be carefully structured to account for the various levels of knowledge and exposure across the organisation's personnel.

It may be shown[7] (Taylor, 1999) that people exhibit differing modes of learning. As such, sessions need to be tailored towards individual focus groups within the organisation. Emotional intelligence[8] is an important guide when deciding on teaching skills. The facilitator in an awareness session needs to balance the political issues at hand carefully, ensuring not to alienate staff. Is important that staff know they are not being victimised.

Information security awareness and training must be included in and attached to the existing induction programmes. Additionally, presentations and refresher courses need to be taught separately. On the job and mentoring programmes are cost-effective methods of implementing training within several roles.

Security awareness is not a comprehensive information security and training programme in itself. Users need to have constant reminders in order to stay focused on information security concerns. A large number of small 30 to 45 minute sessions over time, is preferable to a single session over a whole day.

High-quality training materials are generally received better and digested more thoroughly by an audience. Through working with other organisations, training materials may be shared at a lower cost to both organisations. Other organisations with similar needs should be approached for this purpose.

The programme needs to be developed and implemented along the following lines:

Awareness	What can happen to the organisation?
Training	How can I help?
Education and professional development	Understanding why is this happening.

[7] Taylor, G.J., Parker, J.D.A., and Bagby, R.M. (1999). "Emotional intelligence and the emotional brain: Points of convergence and implications for psychoanalysis". Journal of the American Academy of Psychoanalysis, 27(3), 339-354.

[8] Hay/McBer (2000). "Research into teacher effectiveness: A model of teacher effectiveness report by Hay McBer to the Department for Education and Employment". Report prepared by Hay/McBer for the government of the United Kingdom, http://www.dfee.gov.uk/teachingreforms/mcber/.

© SANS Institute 2000 - 2005 Author retains full rights.

responsibilities on a frequent basis.

Training and education are longer term processes designed to allow users to apply and interpret the information they have received in a manner beneficial to the organisation's information security stance.

All users within the organisation and many external parties that deal with the organisation need to be aware of the organisation security requirements. Training and education on the other hand, are applied selectively to individuals, based on their role within the organisation.

6 Regular maintenance

The rate of change of technology within the information fields drives the need to update any awareness and training programme constantly. Awareness training programmes may become ineffective, as applications are updated or the internal environment is changed.

Further, external requirements such as legislative changes or business partnerships and amalgamations may force the organisation's policy to change or become obsolete. Today's increasingly political nature and the rapid rate of media dissemination make public perceptions an important consideration.

This programme requires a high standard of maintenance because of the visibility of this programme both internally and externally to the organisation. It must also face the current issues of information security affecting the organisation. A failure to do this is likely to result in the weakening of the programme as staff discount IT usefulness.

7 Periodic evaluations

Programme evaluations will be covered in detail later in the document. The ISMS ACT stage covers this in detail. It is important to remember that this programme is cyclic in nature and based on the Plan, Do, Check, Act (PDCA) process. For this reason, the evaluation stage should not be forgotten during planning.

A combination of statistical methods based on the following data should be compiled in order to obtain feedback on the success of the awareness and training programmes:

- Post seminar valuations;
- Periodic mini quizzes to selected employees and departments
- Qualitative and quantitative analysis of information security incidents.
- Audit and review

© SANS Institute 2000 - 2005 Author retains full rights.

Statistical analysis of the reported security incidents across various systems over time may be used as a basis for reviewing the success of the programme.

Policy, Standards and Guidelines

Information security training can and should be used to support all information security controls. By meticulously training all staff, whether designers, management, or general system users, compliance with the organisation's policies standards and guidelines will be more likely to be successfully implemented[9].

Awareness

Awareness of the organisation's policies and procedures is essential in ensuring accountability. All new personnel are to complete information security awareness sessions as a part of their initial induction.

It is a condition of employment that all staff read and understands the information policy procedures and standards as they relate to their role within the organisation. If staff have any issues with this or do not understand the policies, standards or procedures adequately, they are encouraged to discuss these issues with either their manager or the information security manager of the organisation.

It is a condition of employment that all employees sign a document stating that they have read and understood the information security policies, procedures and standards of the organisation. To achieve this it is fundamental that these documents have been made available to them.

Existing staff who have not already signed the acceptance documents will be required to do so at the next bi-annual performance review. Negotiations with unions to ensure the successful implementation of this strategy are to be managed based on organisational need. All existing employees who did not attend awareness sessions when they initially joined the organisation shall be required to attend a session within the next three months.

Additionally, all personal are to complete awareness update sessions on a regular basis. A selected random sample of staff will be regularly tested using a combination of methods such as online quizzing in order to develop a statistical model and plot of the organisation's overall awareness of information security practices.

Whenever information security policy, procedures or standards change or are

[9] Administrative committee on coordination, Information Systems coordination committee (ISCC), "Information security: recommended practices for United Nations organisations", 1994.

© SANS Institute 2000 - 2005 Author retains full rights.

updated, all users affected by the changes need to be made aware of the changes.

Training

Continued training is an essential step in ensuring that all employees are aware of the organisation's policies. The successful completion of an information security and awareness and training programme upon employment is a requirement to be granted access to the computer of systems and network.

Education and Professional Development

The organisation recognises the need for more in-depth security training for security professionals, information management professionals, IT staff and other individuals who may require additional expertise.

To this end, the organisation as part of the employees career development programme will work with the employee to ensure their growth and knowledge through specialised training. This needs to be individually tailored with the individual's manager and the training department being involved in this process. For selected individuals, the maintenance of key certifications and achievement of CPE[10] hours will be written into their employment contract.

Corporate Policy and Standards for Awareness and Training

Policy: User Training

To ensure that users are aware of information security threats and concerns, and are equipped to support organisational security policy in the course of their normal work, they should be trained in security procedures and the correct use of IT facilities.

Hiring

All personnel conducting interviews must have received training in the interviewing process at <the organisation>.

Induction

Induction of new employees at <the organisation> will take place in three stages:

Managers Induction

[10] CPE – Continuing Professional Education

© SANS Institute 2000 - 2005 Author retains full rights.

The new employee will be inducted by their immediate manager or their designate, on the morning of their first day at work on the following topics:

1. The job functions in detail,
2. The responsibilities, including security responsibilities of the position,
3. The performance measurement criteria of the position.

The manager and the employee will sign a statement that the induction did take place. A copy will be lodged with the Human Resources group to be placed on the employee's file.

Human Resources Induction

The new employee will be inducted by the Human resources group on the morning of their first day at work on the following topics:

- Staff Safety to include, fire drills, building evacuation and first aid;
- Security Awareness to include, Information Security Policies sighting and written acknowledgment.

The employee and Human Resources will sign a statement that the induction process was performed. The statement will be lodged in the employee's records.

General Orientation.

Within the first three months the employee will receive a general orientation briefing about <the organisation> coordinated by the Human Resources Group.

Contractors shall be subject to points 1 & 2 from above.

Employment

On an annual basis, all employees and contractors will be re-briefed and where applicable re-sign documents for the following topics:

1. Staff Safety;
2. Fire evacuation;
3. First Aid;
4. Security Awareness.

On an annual basis, all employees are to receive a Performance review from the immediate manager. The review will be performed against performance measurement criteria and with regard to their security responsibilities.

© SANS Institute 2000 - 2005 Author retains full rights.

On selection for promotion or a move to a new position, ensure the completion of all necessary background checks appropriate to the new position prior to the individual commencing in the new position.

Any employee or contractor of <the organisation> must report any suspected or actual breaches of security to Help Desk as soon as possible.

A breach of security will be considered grounds for disciplinary action against the individual and this may include termination.

RESPONSIBILITIES

Employees

Each employee is responsible for complying with the policies and procedures relating to information technology security and for fully cooperating with the IT staff within their division to protect the IT resources of the organisation. HR needs to work with management to ensure that the correct procedures and processes are being followed.

Human Resources must ensure that each employee becomes familiar and complies with the organisations Policy.

Senior Management

Human Resources need to work with senior management to ensure compliance when:

1. Enforcing the policies, standards, procedures, and guidelines for the protection of IT resources and information.

2. The appointment of Computer Support Representatives, and providing appropriate funding, training, and resources to those people for information security-related tasks.

3. Applying sanctions consistent with Human Resources policies to either individuals or department heads that break provisions of this policy. This applies if the breach was enacted wilfully, accidentally, or through ignorance.

4. Designating Data Stewards for each significant collection of business information, who in turn are responsible for determining the value of their information and implementing appropriate security measures as specified in the Data Access Policy

5. Sponsoring internal awareness and training programmes to familiarise employees with the security policy, procedures and recommended practices.

Risk Management

A combination of the Australian standard, “AS4360: Risk Management” and COBIT[11] will be used as our baseline guide to developing a process to mitigate

© SANS Institute 2000 - 2005 Author retains full rights.

undue risk. The stages involved with this standard are detailed in the diagram below.

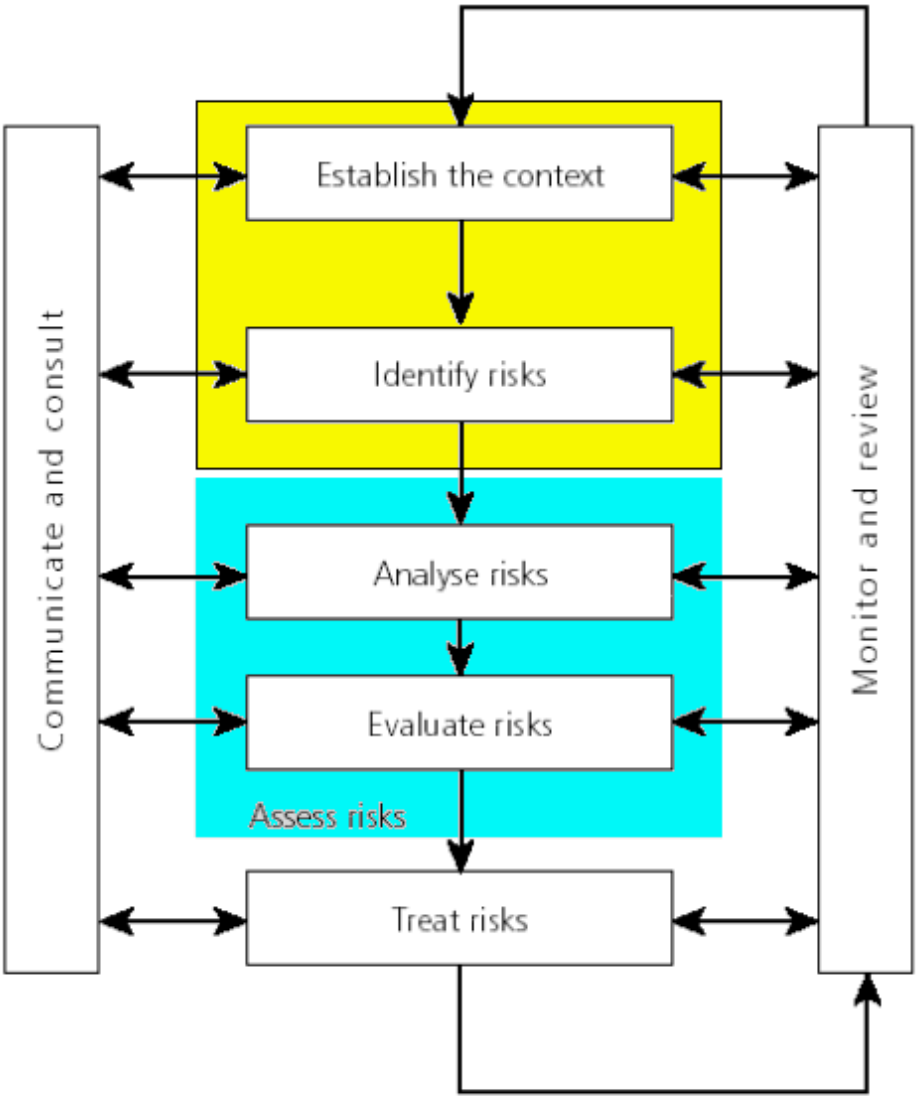


Figure 3 - AS/NZS 4360 - Risk Management Overview

The context of this framework is defined within this document as a whole. As

[11] Ozmen, Kemal "IT Risks and Controls: Risk Identification, Risk Mitigation, Risk Management, Controls Implementation"

© SANS Institute 2000 - 2005 Author retains full rights.

such, the initial stage of this process, while planning the ISMS is the identification of risks associated with this awareness and training process. The two, check, and act phases of the ISMS will details steps to further analyse and evaluate the risks and finally treat any residual risk.

Skills development is a critical factor not only in this training process, but also to all other aspects of the organisational ISMS. Increasing understanding and skills of managers and their staff increases their accountability and the level of responsibility towards the organisation.

Some other methods utilised to deliver training material include[12]:

- Interactive video training and other distance learning techniques,
- Web-based training through the Intranet,
- Non-Web CBT (Computer based training),
- Instructor led training sessions
- Presentations and mentoring.

The procedures defined in this and document involves the completion of the following tasks:

1. Establishing the organisational culture (and the associated risk environment);
2. Identifying the organisation's risks;
3. Analysing the risks as identified;
4. Assessing or evaluating the risks;
5. Treating or managing the risks (using cost / benefit frameworks);
6. Monitoring and reviewing the risks and the risk environment; and
7. Continuously communicating and consulting with key parties.

Some of the key risks associated with this ISMS include:

1. Awareness levels are inadequately raised during either induction activities or subsequent awareness sessions;
2. Policies and procedures are not being updated;
3. Information security training fails to provide staff with an adequate level of skills to handle the security needs of the organisation;

[12] NIST 800-50, NIST 800-16.

© SANS Institute 2000 - 2005 Author retains full rights.

4. Awareness sessions are not adequately focused on the policies procedures and standards of the organisation;
5. Senior management do not support the awareness and training regime adequately
6. Awareness or training activities are not maintained and kept current.
7. Internal politics reduce the effectiveness of the programme.

Failure to mitigate the risk associated with poor awareness and training techniques increases the likelihood and exposure to other risks within the organisation.

It is difficult to enforce controls on systems when staff are either unaware of the requirements or in adequately trained in securing those systems.

Is important to remember that the success of the organisation's information security strategy requires all personnel to have sufficient knowledge of the awareness requirements of the organisation and that key personnel maintain key competencies in their areas of the ISMS[13].

To achieve this is necessary to:

1. Determine the necessary competencies within the organisation,
2. Provide awareness sessions and training for staff,
3. Evaluate the effectiveness of awareness and training sessions on a regular basis,
4. Maintain sufficient training records on the experience skills and qualification of staff to enable the recognition and analysis of weaknesses within the organisation.

Primary Risks and Controls

The techniques used to mitigate the identified risks are detailed below.

[13]Oud, Ernst J. "ISO/IEC 17799 Compliance", "COBIT Security BaselineTM and ISO/IEC 17799 compared", and "Using COBIT for BS 7799-2 compliance audits"

© SANS Institute 2000 - 2005 Author retains full rights.

RISK	Probability of Event	Harm of Event	Risk Calculation	Control (AS 17799) (COBIT)[14]
Inadequate awareness raising during either induction activities or subsequent awareness sessions	Medium 3	Significant 2	Medium 6	3.1.1 3.1.2 4.1.2 4.1.3 4.1.5 6.1.1 6.1.2 6.1.3 6.1.4 6.2.1 6.3.5 **DS1, DS7**
Policies and procedures are not being updated	Low 2	Significant 2	Medium 4	3.1.1 3.1.2 4.1.2
Information security training fails to provide staff with an adequate level of skills to handle the security needs of the organisation	Medium 3	Damaging 3	High 9	3.1.1 3.1.2 4.1.2 4.1.3 6.1.1 6.2.1 **DS1, PO7**

[14] COBIT is developed by the ISACA, http://www.isaca.org

© SANS Institute 2000 - 2005 Author retains full rights.

Awareness sessions are not adequately focused on the policies procedures and standards of the organisation	Low 2	Damaging 3	Medium 6	3.1.2 4.1.2 4.1.3 4.1.5 6.2.1 **PO3, DS7**
Senior management do not support the awareness and training regime adequately	High 4	Serious 4	Critical 16	3.1.1 3.1.2 4.1.1 4.1.2 4.1.4 6.3.5 8.1.4 12.1.5 **PO1, PO10, DS10**
Awareness or training activities are not maintained and kept up to date	Medium 3	Significant 2	Medium 6	3.1.2 4.1.3 4.1.5 6.1.1 6.1.4 **M1, M2**
Inadequate awareness raising during either induction activities or subsequent awareness sessions	Low 2	Serious 4	High 8	3.1.1 3.1.2 4.1.2 6.1.2 6.1.4 6.2.1 **A14, DS13, M1**

© SANS Institute 2000 - 2005 Author retains full rights.

The most critical issue to face the organisation at the current time in respect to Awareness and Training is that of Senior Management Support.

Determination of Results

The following tables where used to determine the risk table above.

Harm of Event	Degree of Harm
Insignificant	Minimal to no impact
Minor	No extra effort required to repair
Significant	Tangible harm, extra effort required to repair
Damaging	Significant expenditure of resources required, damage to reputation and confidence
Serious	Extended outage and/or loss of connectivity, compromise of large amounts of data or services
Grave	Complete compromise, loss of life associated with the event.

Risk Calculation (Probability x Harm)	Rating
0	None
1–3	Low
4–7	Medium
8–14	High
15–19	Critical
20–30	Extreme

Summary of Controls Implemented

Control ID	Details of Control	Description
3.1.1	Information security policy document	Whether there exists an Information security policy, which is approved by the management, published and communicated as appropriate to all employees. Whether it states the management commitment and set out the organisational approach to managing information security.

© SANS Institute 2000 - 2005 Author retains full rights.

3.1.2	Review and evaluation	Whether the Security policy has an owner, who is responsible for IT maintenance and review according to a defined review process. Whether the process ensures that a review takes place in response to any changes affecting the basis of the original assessment, example: significant security incidents, new vulnerabilities or changes to organisational or technical infrastructure.
4.1.1	Management information security forum	Whether there is a management forum to ensure there is a clear direction and visible management support for security initiatives within the organisation.
4.1.2	Information security coordination	Whether there is a cross-functional forum of management representatives from relevant parts of the organisation to coordinate the implementation of information security controls.
4.1.3	Allocation of information security responsibilities	Whether responsibilities for the protection of individual assets and for carrying out specific security processes were clearly defined.
4.1.4	Authorisation process for information processing facilities	Whether there is a management authorisation process in place for any new information processing facility. This should include all new facilities such as hardware and software.
4.1.5	Specialist information security advise	Whether specialist information security advice is obtained where appropriate. A specific individual may be identified to co-ordinate in-house knowledge and experiences to ensure consistency, and provide help in security decision making.
6.1.1	Including security in job responsibilities	Whether security roles and responsibilities as laid in Organisation's information security policy is documented where appropriate. This should include general responsibilities for implementing or maintaining security policy as well as specific responsibilities for protection of particular assets, or for extension of particular security processes or activities.

© SANS Institute 2000 - 2005 Author retains full rights.

6.1.2	Personnel screening and policy	Whether verification checks on permanent staff were carried out at the time of job applications. This should include character reference, confirmation of claimed academic and professional qualifications and independent identity checks.
6.1.3	Confidentiality agreements	Whether employees are asked to sign Confidentiality or non-disclosure agreement as a part of their initial terms and conditions of the employment. Whether this agreement covers the security of the information processing facility and organisation assets.
6.1.4	Terms and conditions of employment	Whether terms and conditions of the employment covers the employee's responsibility for information security. Where appropriate, these responsibilities might continue for a defined period after the end of the employment.
6.2.1	Information security education and training	Whether all employees of the organisation and third party users (where relevant) receive appropriate Information Security training and regular updates in organisational policies and procedures.
6.3.5	Disciplinary process	Whether there is a formal disciplinary process in place for employees who have violated organisational security policies and procedures. Such a process can act as a deterrent to employees who might otherwise be inclined to disregard security procedures.
8.1.4	Segregation of duties	Whether duties and areas of responsibility are separated in order to reduce opportunities for unauthorised modification or misuse of information or services.
12.1.5	Prevention of misuse of information processing facility	Whether use of information processing facilities for any non-business or unauthorised purpose, without management approval is treated as improper use of the facility. Whether at the log-on a warning message is presented on the computer screen indicating that the system being entered is private and that unauthorised access is not permitted.

© SANS Institute 2000 - 2005 Author retains full rights.

Information Assets

The information assets associated with the ISMS includes:

- Internet and intranet tools and methodology for use within the organisation;
- The Help Desk service,
- The incident response system,
- Awareness and training materials and processes for personnel in each stage of implementation,
- Specialist advice and the mentoring of internal staff and professional risk advisers.

It is important that the training materials and associated information assets of this ISMS be maintained to a current and relevant state at all times. Training materials include any videos, newsletters, posters, lecture notes, survey results, etc.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

3. Do, "Implement and operate the ISMS"

The "Do" phase and involves a gap analysis and creation of the mitigation strategies for the awareness and training programme. It is important to ensure that the awareness and training programme includes all members of the organisation[15]. The employees need to understand and respect the practices of the organisation and IT drive to improve security.

The organisation's personal are the first line defence against information security violations[16]. If the organisations personal are adequately trained, they can not only help prevent incidents from occurring, but also reduce the impact when an incident does occur[17].

Well-designed, consistent awareness sessions on a regular basis, will develop the instinctive security response within employees. For this to be achieved, the appropriate resources, including people time and money need to be made available. Is important that the controls of all sections of the ISMS be documented adequately and that documentation maintained. If the other controls within the organisation are not documented correctly, the success of the awareness and training programmes will be lessened.

The primary aim of an awareness programme is to instil an appropriate understanding of risk and develop a security conscious culture within the organisation. The security awareness programme will only be successful if it is continuously monitored to ensure IT continual effectiveness and relevance to the organisation. Training and education programmes that are more specific will support the awareness programme, and thus help members of the organisation maintained the security of the organisation.

Problems, Actions and Steps

[15] McLelland, Ross (2004), "emotional intelligence in the Australian context", Pacific Consulting, http://www.pacificconsulting.com.au/articles_ei.htm

[16] Katzke, S, "A Government Perspective on Risk Management of Automated Information Systems", Proc. 1988 Computer Security Risk Management Model Builders' Workshop, NBS, Gaithersburg MD, USA, 1988.

[17] D. Pottas , Sebastiaan H. von Solms, Superseding Manual Generation of Access Control Specification - From Policies to Profiles, Proceedings of the IFIP TC11, Ninth International Conference on Information Security: Computer Security, p.327-342, May 12-14, 1993

© SANS Institute 2000 - 2005 Author retains full rights.

More effort has been focused on the awareness programme then the training programme in this document. This does not imply that training is any less important. Individual training sessions will be based upon individual departmental and staff needs. Awareness on the other hand, is critical for the entire organisation as a whole.

Separate training and education programmes need to be worked out and developed for individuals, departments and functional roles as required to support the controls of the overall organisational ISMS.

Awareness Programmes need to be implemented

Management can facilitate awareness, training and education strategies with the organisation. Good awareness processes and management support will help in the overall security of an organisation as:

1. An organisation's personnel can not be held responsible for their actions unless it can be demonstrated that they were aware of the policy prior to any enforcement attempts,

2. Education helps mitigate corporate and personal liability, avoidance concerning breaches of criminal and civil law, statutory, regulatory or contractual obligations, and any security requirement,

3. Awareness training raises the effectiveness of security protection and controls; it helps reduce fraud and abuse of the computing infrastructure and increases the return on investment of the organisation's spending on both information security as well as in computing infrastructure in general[18].

As in most organisations, the level of education required, as well as the need for good security controls and procedures have fallen way behind the requirements. Users of information systems often see security processes as punitive and unnecessary. Developers see controls as restrictive and counterproductive in their efforts to develop and introduce systems.

An initial security awareness workshop developed at management level for the security personnel and the security governance team is a good initial phase with which to identify business requirements, the security key threats and perils that

[18] "The human firewall", Abby Christopher, 28/10/2003

© SANS Institute 2000 - 2005 Author retains full rights.

must be addressed, and to develop a management plan to meet these new challenges.

Security Awareness Workshops

The initial phase in the development of this workshop is to identify and invite key client participants to be involved in the process. These business and management representatives will then:

- Engage in defining the current and planned business activities,
- Define for each activity the security threats and perils to be expected,
- Each activity to the relevant security requirements,
- For each activity, review the relevant controls.

It is important that these recommendations be reviewed regularly against short and long-term management objectives to maintain and improve the awareness process.

Results of the security workshop

From the initial security workshop, the ISMS management team should have an idea of the;

- Objectives
- Business corrections and security requirements
- An overview of threats and risk faced by the organisation
- Highlights of the major strengths and weaknesses of the organisation from an information security perspective

This will allow the security management team to develop a set of business-orientated recommendations, which may be used to develop the security awareness programme.

What Is Information Security Awareness Training?

Security awareness training is a training programme aimed at heightening security awareness within the organisation. Simply stated, the training aspects of an effective security awareness programme should result in:

© SANS Institute 2000 - 2005 Author retains full rights.

- A detailed awareness programme tailored to the organisation's needs;
- Heightened levels of security awareness and an appreciation of information assets;
- A reduction in the support effort required by the organisation.

A security awareness programme should be an ongoing programme as training tends to be forgotten over time. As people face more pressure for increased productivity, they tend to look at security as time consuming and a hindrance and tend to find ways to circumvent security. Even without the pressure, most people tend to relax towards their responsibility of following procedures and guidelines unless they are periodically reminded of it.

The US security hearings[19] following the 911 incident and the ensuing actions in the subsequent years emphasise how individual senses are heightened after an incident. This is no different for an information security related event. It needs to be remembered that awareness will rise after an event, but that this is short lived without reinforcement.

Description and scope

The introduction of security awareness sessions will:

- Demonstrate senior management's commitment to information security;
- Encourage middle management to motivate other employees to adopt "Good Security Practices";
- Improve processes required to support security administration and maintenance and user access requests;
- Heighten acceptance of security processes and provide for increased productivity and more effective use of information systems by all users

[19] "HOMELAND SECURITY", HEARINGS before the COMMITTEE ON APPROPRIATIONS UNITED STATES SENATE ONE HUNDRED SEVENTH CONGRESS SECOND SESSION, SPECIAL HEARINGS, APRIL 10, 2002--WASHINGTON, DC, APRIL 11, 2002--WASHINGTON, DC

© SANS Institute 2000 - 2005 Author retains full rights.

while providing a greater sense of shared accountability for the security of the organisation's information assets;

- Provide additional benefit in the flow on effect of the way in which employees relate to other work Processes and will provide them with a greater sense of ownership;
- Save costs by reducing the number of errors made; and
- Improve communication processes within the organisation.

Method

The best approach to use for the introduction of the security awareness training will:

- Select a section that can be used for the pilot study;
- Conduct the awareness workshops commencing with the employees;
- Seek feed back by way of a workshop appraisal questionnaire;
- Modify the awareness programme if required;

There should ideally be a follow up awareness questionnaire four weeks after the programme is completed to ascertain the programmes level of success and provide input for further modification if required for future workshops.

Time Scales

Given that class sizes should not be greater than 20 – 30 people to allow for effective communication amongst the group, and that each session should take no more than 2 – 3 hours, the entire staff could be covered in a number of weeks[20] using a system of rolling lectures.

[20] This is dependant on the size of the organisational unit as well as staff availability.

© SANS Institute 2000 - 2005 Author retains full rights.

Security Awareness Resource Requirements

Management need to review the Security Awareness Training programme to monitor the progress of the implementation of the awareness programme.

A basic need in this exercise is to ensure that the security recommendations are transmitted into actions. In other words, the message must be simply presented in a memorable way so that these actions are everlasting. A definite and permanent change in attitude must result from this project.

To help in this change, management need to monitor the progress and effectiveness of security awareness training by constantly reviewing the violation reports and type of inquiries received.

Training Programmes need to be developed

Training programmes shall be designed and developed following the seven step approach of the CSAT[21] programme.

Step one	identify programmes scope, goals and objectives
Step two	identify training staff.
Step three	identify target audiences.
Step four	motivate management and employees within the organisation.
Step five	administer the programme.
Step six	maintain the programme.
Step seven	evaluate the programme.

The CSAT process maps closely to the ISO 17799 process. The seven steps above map closely to Plan, Do, Check, Act processes of an ISMS.

The goals and objectives of the programme are to sustain appropriate level of protection for the information resources of the organisation. Specific training goals must be defined to meet individual departmental and employee

[21] "Computer Security Awareness Training and the Interactive Learning Framework", By McDonald Bradley, Inc. January 10, 2002

FISSEA 2003 Annual Conference: "Securing Your Cyber Frontier Through Awareness, Training and Education" Agenda and Presentations - March 4-6

NIST SP 800-12, Chapter 13

© SANS Institute 2000 - 2005 Author retains full rights.

development requirements.

Depending on the needs of the organisation and the availability of suitable resources, training staff may be selected from internal training departments, information technology staff, or external contract services.

Depending on the needs of the organisation, training may be segmented based on the technology and systems used, functional roles or job categories, the user's level of knowledge or even by the needs of a specific project.

It should be remembered that both management and employees could have separate agendas. Often the best motivation for management is an awareness of the possible losses and damage to the organisation of which a security breach may result. Employees need to know that information security is a valuable aspect of their roles and that it is important for the continued well-being of the organisation.

Training materials and courses should be tailored towards the needs of the audience. It is important to maintain a high quality in training materials even if this means obtaining and modifying material from other sources.

The training programme needs to be constantly updated due constant changes within the industry. Not responding to change would quickly make the programme obsolete.

Changes and updates to systems, applications and the general organisational environment occur at a frequency that pushes constant change. Failure to maintain the training process will quickly result in vulnerabilities to the organisation.

A combination of quantitative and qualitative statistical methods should be used to evaluate the effectiveness of the programme.

Cost Considerations

The funding requirements for the development of the awareness and training programmes include:

- Costs associated with developing and maintaining the materials;
- The costs, from both at the venue and staff time and other ancillaries of providing the sessions;
- Expenses including external training courses, consultants; and
- Materials such as books and documents used in the courses.

Statements of Applicability

© SANS Institute 2000 - 2005 Author retains full rights.

Control ID	Description of Control	Implementation or Justification	Method	Comment
3.1.1	Whether there exists an Information security policy, which is approved by the management, published and communicated as appropriate to all employees. Whether it states the management commitment and set out the organisational approach to managing information security.	Implementation is underway	The security committee as a government mandate to implement policies. The team has been selected to review and update these documents.	This process is well underway.
3.1.2	Whether the Security policy has an owner, who is responsible for IT maintenance and review according to a defined review process. Whether the process ensures that a review takes place in response to any changes affecting the basis of the original assessment, example: significant security incidents, new vulnerabilities or changes to organisational or technical infrastructure.	Implementation is underway	Processes are being developed to ensure all policies and standards have owners. Existing policies have been assigned to key personnel.	An organisational CIO has been selected and given authority over this task.

© SANS Institute 2000 - 2005 Author retains full rights.

6.2.1	Whether all employees of the organisation and third party users (where relevant) receive appropriate Information Security training and regular updates in organisational policies and procedures.	Implementation is underway	Proposed awareness sessions and training schedules, and been developed and are being tested.	Details proposed awarenes s sessions are included in this document.
8.1.4	Whether duties and areas of responsibility are separated in order to reduce opportunities for unauthorised modification or misuse of information or services.	Not fully Implemented Inadequate funding and staff. Other controls are in place.	N/A	N/A

© SANS Institute 2000 - 2005

© SANS Institute 2000 - 2005 Author retains full rights.

4. Check, "monitor and review the ISMS"

A critical factor to the continued success all security awareness and training programmes is the process of constant maintenance and re-engineering such that they are both are relevant and compliant with the organisation's objectives.

As is stated in NIST special publication 800-50, "continuous improvement should always be the theme for security awareness and training initiatives, as this is one area where *you can never do enough*."

A comprehensive audit plan[22] needs to be developed and maintained with any organisation. This plan needs to address the controls detailed below.

Training Audit and Checklists

Control ID	Reason for Control	Checks Used to Audit and Maintain the Controls
3.1.1 Information security policy document	The information security policy provides management direction and support for information security. This document sets a clear direction and demonstrates management support and commitment to information security through this policy.	The primary checks used include the testing of the existence and relevance of the policy. A review of how policies are disseminated within the organisation and the extent of signed acceptance forms should be completed at least annually. This will occur more frequently within certain departments.

[22] "EDUCATION AND TRAINING", Guidance Notes on the application of ISO 9001 for quality management systems in Education and Training, BSI, Revised 1999.

© SANS Institute 2000 - 2005 Author retains full rights.

3.1.2 Review and evaluation	For a policy, process or standard to be effective and for it to be adequately advertised within the organisation, it is important that it has assigned an owner who will maintain it effectively.	All policy standards and processes need to be reviewed at least quarterly to ensure that the controls over ownership are effective. Processes are being developed to ensure all policies and standards have owners. Existing policies have been assigned to key personnel. The ownership of the awareness and training policies needs to be reviewed to ensure appropriateness.
4.1.1 Management information security forum	The management information security forum is responsible for insuring the effectiveness of the awareness and training programme for the organisation.	Control should be implemented review the membership of this forum, to review the roles and responsibilities of the members within the forum, and to ensure that the meetings are being attended by the members on a regular basis. Is important that the awareness of the members of the team be evaluated periodically. Foreign members should be interviewed periodically to ensure that they remain aware of the organisation security requirements.

© SANS Institute 2000 - 2005 Author retains full rights.

4.1.2 Information security coordination	Is important that members from across the organisation be involved in the security process. Awareness of security issues is critical to all aspects of the organisation. For this reason, management representatives need to be selected from across the divisions.	Review of the membership of this team needs to be completed periodically to ensure that the members reflect the broad goals of the overall organisation. Quantitative data, reflecting the number of incidents within the organisation may be used to gauge a level of awareness, using statistical means, throughout the organisation.
4.1.3 Allocation of information security responsibilities	Is crucial to ensure that employees are fully aware of their security responsibilities to the organisation and that these responsibilities have been allocated effectively.	A review of critical roles through HR should be conducted at least quarterly. A general review of operational roles, compiled by the individual departmental managers needs to be completed annually in conjunction with HR.
4.1.4 Authorisation process for information processing facilities	It is important that managers and systems owners understanding the requirements for authorisation and other controls.	An annual evaluation, coordinated between HR and internal audit should be done on selected samples within the organisation to determine if effective levels of authorisation are being implemented across systems.
4.1.5 Specialist information security advise	As it is not feasible to retain all possible skill sets within the organisation, external specialists will be retained from time to time. It is important that the engagements, conducted by these specialists be reviewed periodically to ensure that they are both relevant and effective for the organisation.	Interviews with key staff and system owners should be conducted at the completion of all external engagements. Qualitative of surveys of systems owners and personnel within the organisation should be conducted on a periodic basis to evaluate the performance of parties contracted to provide specialist information security advice.

© SANS Institute 2000 - 2005 Author retains full rights.

6.1.1 Including security in job responsibilities	Helps to reduce the risk of human error, theft, fraud or misuse of facilities. Security should always be addressed at the recruitment stage and included within job descriptions and employee contracts. It is important to monitor security during an individual's employment.	KPI's, employee contracts and policies should be reviewed. This is especially important for sensitive jobs. A check that all employees and third-party users of the IT facilities have signed confidentiality agreements and other required documents should be conducted.
6.1.2 Personnel screening and policy	This check reduces the risk associated with personnel accessing sensitive information is using that access.	A check of least to satisfactory character references including one business and one personal should be completed. Samples of employee CV's may be checked to ensure that HR has confirmed academic and professional qualifications, and the accuracy of the employees CV.
6.1.3 Confidentiality agreements	This control is required to reduce the risk associated with employees are abusing the confidentiality of the organisation's data. This agreement helps raise the awareness of this issue.	Check that the appropriate confidentiality agreement has been signed. It is important to check that users have re-signed these documents. If they have been updated or changed.
6.1.4 Terms and conditions of employment	This control helps users become aware of the conditions are so shared with their employment and reduces the risk of those employees intentionally bypassing controls.	Is important to make the terms and conditions of employment clear and unambiguous. By including the security requirements of employment in the terms document uses a less likely to be unaware of the requirements.

© SANS Institute 2000 - 2005 Author retains full rights.

6.2.1 Information security education and training	This control helps ensure that security procedures are correctly followed. This minimises the security risk to confidentiality, integrity and availability of the services through user error.	Testing and samples should be obtained through the awareness programme and quizzes within the organisation to evaluate the awareness levels.
6.3.5 Disciplinary process	It is important that there is a formal disciplinary process for employees who were allegedly violated. The organisation security policies and procedures. This process acts as both a deterrent to employees who might be inclined to disregard procedures, and helps ensure correct and fair treatment for employees who are suspected of committing a serious breach.	The process should be reviewed for consistency and to evaluate IT effectiveness on a regular basis. A review a review of the policy should be completed periodically. A qualitative survey from a representative sample of the organisation's employees should be conducted at least every six months to determine the levels of awareness and effectiveness of this process.
8.1.4 Segregation of duties	Ensuring a segregation of duties for critical systems reduces the risk of unauthorised systems modifications and access to data.	This control requires a review of the organisational roles and responsibilities to ensure that key positions within the organisation have at separation of duties on critical systems.
12.1.5 Prevention of misuse of information processing facility	Is important that users are aware of their roles in order that they operate within the organisation's guidelines.	A review of the awareness process and need knowledge of the users should be conducted at least quarterly. A quantitative analysis of incidents within the information processing facility should be reviewed monthly to ensure that the level of incidents at least remained static, or ideally decreases.

System Improvement Monitoring and Checks

The aim of this programme is continuous improvement in the organisation's

© SANS Institute 2000 - 2005 Author retains full rights.

security awareness, training, and education levels. The process of securing the organisation's information infrastructure requires continuous teamwork. "We'll have to work together, or we all fail together."

In order to ensure this programmes success, we need to be able to monitor the following key areas using appropriate metrics:

1. Approval for adequate funding has been obtained,
2. Senior management supports and evangelises the programme
3. Organisational metrics indicate a reduction in the number of incidences and security violations[23] within the organisation,
4. IT personnel and management do not use their position to bypass security controls,
5. The level of attendance security meetings and sessions is increasing, rather than decreasing,
6. The percentage of appropriately security-trained personnel has increased.

Some additional testing to evaluate the level of user awareness in the organisation will include:

1. Random "spot checks"[24] of behaviour to determine if workstations are logged in while unattended, if confidential media is not adequately protected, etc.
2. Web-based media on the intranet will be configured to record the userid when it is accessed. This will allow the audit department to check, what percentage of the organisation has been accessing this material, and what level of comprehension they are retaining.

[23] It would be expected that the number of security incidents reported would increase with the measured levels of awareness in the organisation. Detailed qualitative and quantitative measures may need to be developed.

[24] Privacy is a concern with this activity. It is important that all staff have read and aware of the organisation's privacy policy and that they have signed and accepted these policies.

© SANS Institute 2000 - 2005 Author retains full rights.

3. A selection of password cracking programmes will be run on the monthly basis to ensure that employees are following the organisational policy on password length and complexity.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

5. Act, "maintain and improve the ISMS"

For the programme to remain effective, the process of continual improvement must be implemented.

A variety of parties must be involved in the on going assessment of the awareness and training programme.

- **Senior management** – need to provide support through strategic planning. The support of senior management is critical to the success of these programmes. Through evangelising the programme, senior management helps ensure the programme's uptake and success.
- **Information security manager** – can help identify training sources, evaluate the effectiveness of awareness and training programmes evaluate vendor based and other training sources and aid in the development of awareness and other training materials.
- **Human resources** – need to ensure that awareness and training requirements are established within the organisation's position descriptions, instigate and maintain security focused KPI's for all staff, and ensure that staff receive effective professional development services.
- **Training department personnel** – need to assist in developing overall training strategy, to identify training sources, and aid in the provision of awareness and training sessions.
- **Internal audit department** – the internal audit department needs to monitor compliance with the security directives and overall policy to ensure IT effectiveness. It is important that the internal audit personnel communicate these results effectively.
- **Finance department** – the finance department should use results and feedback from various other sources to a system budget enquiries, help with financial planning, and to provide reports to senior management and other parties on the funding of awareness and training activities.

© SANS Institute 2000 - 2005 Author retains full rights.

System Maintenance

The "Check" phase of this ISMS needs to provide an effective evaluation and feedback in a manner, which will allow a process of continuous improvement. Some approaches to solicit feedback detailing the programme include:

1. **Initiation of an external audit process**, an independent external body may often provide additional insights to the process.
2. **Status reports from management**, individual management has a day-to-day knowledge of the needs of the organisation from a smaller scale viewpoint. A compilation of these manager reports to help improve the overall organisations security standards.
3. **programme benchmarking**, benchmarking (either internal or external) is an effective method of rating the programme both against internal standards as a measure of continuous improvement and as a method of obtaining a rating against one's peers to develop an overall view of the programmes effectiveness.

It is important to remember that the awareness and training programmes are an important subsection of not only the overall information security strategy, but also are a key component of the organisational business strategy as a whole.

As such, quantitative measures need to be implemented and reported on a regular basis such that the effectiveness of the programme may be measured. Some of these stages include:

1. An evaluation of the end user satisfaction towards the awareness sessions and training,
2. An evaluation of the contribution of the awareness sessions and training for the organisations,
3. A process to test the successful transfer of knowledge , and
4. The update process, which is implemented whenever there are changes and new elements, needs to be evaluated for effectiveness.

Some other questions to ask include:

© SANS Institute 2000 - 2005 Author retains full rights.

1. Are the skills required by the personnel working on information security adequate / current,
2. Is the training appropriate for the organisations needs and, is it necessary to hire experienced staff for specific tasks,
3. What is the quantitative efficiency of training and actions undertaken;
4. Is there a current register of education and training for each employee as well as their abilities, experiences and qualifications within the organisation?

Where Next?

Further development in awareness and security training would involve the creation of an organisational skills inventory and the development of a comprehensive knowledge base.

© SANS Institute 2000 - 2005, Author retains full rights

© SANS Institute 2000 - 2005 Author retains full rights.

Conclusion

Our people are our first line of defence. The successful implementation of this ISMS is critical to the success of the entire information security programme.

This paper details the procedural steps needed for the development of an ISMS focused on the provision of security awareness and training systems within the organisation.

The steps used in this document mirror the ISMS process and include:

1. The definition of the system scope,
2. The creation of a project plan,
3. The dedication of the management structures needed for this ISMS,
4. Development of a high-level policy,
5. Asset classification and identification,
6. Risk management and mitigation processes,
7. A gap analysis,
8. A risk-based plan to improve the system based on any gaps found,
9. an audit based checking system,
10. The implementation of the process of continuous improvement.

This is just one stage in the ultimate goal of obtaining ISO 17799 compliance.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Appendixes

Appendix A, Detailed trainer guide for conducting the awareness workshops

Introduction

This guide is intended for use by trainers responsible for the introduction of the concepts, principles, and practices of information security to the users of information systems throughout an organisation.

This workshop is the primary vehicle of a programme to introduce security awareness to an organisation. It forms a significant element of the stream of activities that together comprise a programme designed to cause a major and permanent change in attitude towards information security.

Definition of Workshop

The central and most important aspect of this programme is that it is not to be conducted as a lecture where participants are "force fed" the information. In all presentations of the Security Awareness material those taking part must be made to feel comfortable about presenting ideas and questions for discussion, explanation, or description.

It is for this reason that the term workshop has been deliberately chosen. These presentations must not be lectures dominated by the presenter. In a workshop, the ideal mix is one where at least 50% of the input is provided by the participants.

The material for the workshops is presented with an emphasis on encouraging examples from the working experiences of the participants. Each slide should be used by the presenter as a vehicle for promoting some ideas, experiences, or questions from the participants.

As previously noted, it is important to remember that all staff members exhibit different learning behaviours. An organisational review of the emotional intelligence levels of the staff and trainers may be warranted.

Each workshop is planned to last for approximately 2 - 3 hours and involve between 10 - 20 people. Presentations to groups larger than this will make it very difficult to allow participation for all. In large group workshops, a small group will often monopolise the conversations allowing others to "free-wheel". If the presentation is to contribute to "a major and permanent change in attitude", it must at least be a memorable experience.

In these workshop presentations, we must minimise the "hearing" and maximise

© SANS Institute 2000 - 2005 Author retains full rights.

the "reading" and the "doing". Participants must be motivated, in both the middle management and user presentations, to take a professional attitude towards information security.

The Workshop Outline

The following topics and approximate timings to be covered by the workshop are detailed below.

TOPIC	*TIMING*
An outline of the objectives of the workshop	10
Introduction to the concept of an "Information Asset	10
An explanation of "Information Security	10
Information vulnerabilities; accidental, mischievous, and malicious; Destruction, modification, and theft/copy.	30
Introduction to the organisation and IT policies: Information Security Policy; Information Security Standards; Information Security Procedures;	30
Discussion of security breaches and the subsequent consequences	30
Users role in ensuring good security	30
Conclusion and summary	15
Questions	15

Guidelines for use of tools

A sample of proposed overhead projector slides has been prepared to accompany this report and a text outline of the content that appears follows. They cover all of the topics mentioned above and can be utilised as the main presentation aid in conducting the seminar/workshop. This content is only a recommendation.

To conclude the workshop, attendees should be asked for any suggestions that they may have in relation to any aspect of the Security Awareness Training programme, including slogans, posters or Good Security Practice, ideas should be asked for both at the workshop and at any time in the future.

© SANS Institute 2000 - 2005 Author retains full rights.

Conclusion

It is imperative that senior management realises that security awareness is an ongoing exercise and will require resources to continue the work started by this project. The role of the Information Security Steering Committee must not be underestimated in the influence it can wield regarding the maintenance of a corporate consciousness in this area.

A combination of both reward and punishment is effective in reinforcing the organisation's stance concerning the protection of its information.

Refresher courses should be considered every 12 - 18 months and various promotional efforts must be considered at least every six months to ensure that the message remains fresh and clear.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Appendix B, Example slide content

The following has been designed for use in creating a security awareness programme within the organisation.

Introduction - Slide 1

Background

These workshops were borne of a desire of executive management to improve the level of security awareness within the organisation; this affects the productivity and efficiency of all users of information systems. IT staff continually has to explain and justify security practices. This ties up valuable resources that could be more effectively utilised reviewing business practices and security controls, providing optimum levels of security for the organisation while allowing employees to perform their job functions adequately without any unnecessary barriers.

Employees need to be aware of what constitutes an information asset or what their legal obligations are. It is not commonly understood that the organisation is the legal owner of IT information and that the computer programmes it develops are IT intellectual property not the individuals. Awareness not only protects the organisation, but also the employee.

In most organisations the education required, the criticality of information systems and the need for good security controls and procedures have fallen way behind. Users of information systems often see security processes as punitive and unnecessary. Developers see controls as restrictive and counterproductive in their efforts to develop and introduce systems.

The presentation today will:

- Discuss the issues facing the organisation
- Look at the broader definition of the concept of information and Information Security.
- Examine the threats facing the organisation and possible motives and how other organisations tackling security in the rapidly changing world of information technology.
- Introduce the documentation being produced for protecting information.

© SANS Institute 2000 - 2005 Author retains full rights.

- In addition, look at the ways in which you can help in securing organisation information assets, which will ensure the organisation is better positioned to meet the challenges of information security now and in the future.

- Contain a discussion on security breaches and some of the consequences for you, your colleges and the organisation of security breaches.

You are welcome to take notes but the workshop handouts do include comments made on a reduced version of the presentation slides.

What are the issues - slide 2

What are the issues?

Some of the issues that need to be considered are:

Dependence on Information Systems for Business Continuity

Organisations are becoming increasing dependent on their information systems in order to function effectively. Therefore, the availability of their information systems, the integrity of their data and the confidentiality of corporate information are becoming critical.

Most of the processes we undertake are directly affected by the availability of computer systems. The organisation relies on the availability and accuracy of IT information systems in order to support IT key business functions and to maintain IT level of service to IT customers and dealers.

Information Processing Is No Longer Centralised

Information processing is no longer centralised in one spot and it is therefore more difficult and complex to secure these systems physically and logically.

- Information processing is no longer centralised

- Information processing has moved from a centralised easily controlled large mainframe environment located in one physical location out onto the desks of employees. Computers are in many Australian homes and our own children probably know more about computers than we do!

© SANS Institute 2000 - 2005 Author retains full rights.

- The proliferation of personal computers has revolutionised the availability of computing power and many of companies are moving towards distributed processing where the mainframe is used mainly as a central database.

- Spreadsheets and personal Databases often contain sensitive materials.

- This has however posed a considerable challenge of ensuring the integrity and availability of the information on which organisation depends on to service IT business units, as decentralisation of these computing resources has placed the burden of accuracy, security and control of information on you.

- The traditional approach of combined logical and physical controls that typically apply to mainframes can no longer be applied to protect all information assets. A different approach is required in tackling the challenge of information security in the new millennium.

Greater Exposure to Accidents

There is also the human element

Employees need to be aware of what constitutes an information asset and what their legal obligations are. It is not commonly understood that the organisation is the legal owner of IT information and that the computer programmes it develops are IT intellectual property not the individuals.

Legal requirements

There are various legal requirements that are incumbent on businesses such as this organisation and you as employees for ensuring the law is upheld. Some are common to all businesses such as the confidentiality of tax file numbers, financial and personnel data. There are also other issues such as software copyright where breaches of this act can result in significant fines for the organisations and individuals concerned.

What is information - slide 3

Before we even start taking about security however it is important that we all understand the definition of information.

© SANS Institute 2000 - 2005 Author retains full rights.

Trainers Note: First seek definition from the attendees, write them on a white board or butchers paper, then add any others from the list below that they do not mention.

- Raw data
- Word-processing
- Output reports
- Electronic Mail
- PDA's and Smart Phones
- Programmes
- Records
- Communicated
- Faxes
- Voice Mail
- Web Pages
- Recorded on Diskettes Cartridges
- Spoken and written word

Information is now considerably more portable and more accessible. Imagine trying to carry a four-drawer filing cabinet in your briefcase or handbag, when it can all be contained on a CD or even a memory stick. Imagine trying to lug the cabinet from office to office and across the city, this can now be achieved via the Internet in seconds / minutes across the world.

Information also takes the form of technical diagrams such as networks and programmes specifications. Imagine how useful that would be to someone who wanted to disrupt the organisation.

What is information security - slides 4 - 6

What Is Information Security

There is a common misconception that security processes were developed specifically to make our working lives more difficult and to increase the sales of blood pressure tablets! Nothing could be further than the truth.

Information security is in essence the methods used in protecting information assets from accidental or deliberate:

- Modification,

© SANS Institute 2000 - 2005 Author retains full rights.

- Disclosure,
- Destruction,
- Denial, at a reasonable cost.

It is also concerns the protection of employees and the administration of controls that protect the innocent from unwarranted suspicion. Methods used to protect information assets can be defined as; hardware, software, policies, and procedures appropriate to the classification of assets.

Security of information assets can only be achieved if there are effective security mechanisms within the computer system, at the user interface and throughout the organisation in which the system operates. The approach to information security cannot be piecemeal.

It is important that there are appropriate controls for handling the information whether it is on the computer, through telecommunication lines, faxes, or the handling of printed output. Consideration should also be given to the confidentiality of the spoken and written word. This may seem obvious, but due to the wide spread use of personal computer systems, PDA's or Smart Phones, we now have visual access to considerably more information than we previously had.

Threats - slide 7

Information such as strategic, administrative and financial concerning organisation, products, services and personnel, has always been a vital resource for organisation. However, never before has it been more relied upon or more vulnerable. It is vulnerable because employees are unaware of the value of the information to the organisation and directly for their own job security. It is also vulnerable to the business criminal and those who wish to do organisation harm.

In discussions about security, the question is asked, *what are the threats to organisation*?

Well actually, there are quite a number of threats and these can be broken down into three groups:

- Environmental
- Natural
- Human

© SANS Institute 2000 - 2005 Author retains full rights.

- Internal
  - Errors and omissions
  - Disgruntled employees
- External
  - Competitors
  - Current
  - Potential
  - Organised Crime
  - Political Terrorists
  - Hackers
  - Pressure/Minority Groups

Threats – slide 7 - 9

Internal

Internal threats are just as serious, potentially more devastating and more likely to occur.

Errors and Omissions

While the threats of deliberate action against the company are real and understood, Studies show that large dollar loses for an organisation are from human errors, accidents and omissions. Loses through errors accidents and omissions can comprise:

- changing the production version of a programme instead of the test because the system allows you to do it;
- change a customer details by mistake; and
- introduction of a virus onto the local area network;
- Losing diskettes;
- Careless disposal of sensitive waste;
- Poorly designed systems;

© SANS Institute 2000 - 2005 Author retains full rights.

- Failing to copyright a proprietary programme;
- Inadequate training on the use of information systems.

The rate of errors, omissions and accidents has increased with the introduction of distributed processing because of the lack of understanding in the value of the information and awareness in the correct procedures for handling company information.

Disgruntled Employees

In the area of human threats, it is acknowledged that a small percentage of people are either totally dishonest or honest. For the greater majority of people it just depends on their circumstances and the opportunities presented. Factors, which could affect their honesty, could be; severe financial constraints with one or more partners[25] being made redundant, succumbing to drug or alcohol dependencies or being effected by gambling debts. Loses through deliberate intent can be through the following:

Stealing computer equipment;

- Stealing information which could gain a competitive advantage;
- Taking advantage of loopholes in a financial system;
- Bomb or fire attacks;
- Deliberate introduction of a virus to cause disruption;
- Severing communications cabling ;
- Changing input files to gain financial advantage;
- Stealing a USERID and password for later use to avoid accountability.

Copying company information is easier to do and easier to conceal on computer media than photocopying.

[25] Support of Family Members with problems can equally affect the employee.

© SANS Institute 2000 - 2005 Author retains full rights.

Former employees who have left under a cloud and have knowledge of loopholes also pose a threat and could exploit them to cause disruption or malicious damage.

Threats – slides 10 – 14

- External
  - Curious Crackers
    - Just poking around to see what they can get into
  - Vandals
    - System downtime
    - Network Outages
    - Telephone line use
  - Accidental data disclosure
    - Employee privacy rights
    - Client privacy rights
  - Intentional data disclosure
    - Client privacy rights
    - Damaging to the organisation

Threats - slide 15

Environmental/Natural

Environmental

- Includes both natural disasters and other environmental conditions.
- These threats can result in the loss of availability leading to,

1. Incorrect decision making;
2. Loss of public confidence in the organisation;
3. Financial losses;

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

4. Legal liability;

5. Just to name a few consequences.

- The health and safety of staff may be adversely affected.

- Confidentiality measures may be breached.

Threats - slide 16

Natural

The threat of natural disasters in Australia is a real one and recent example includes:

- Large Insurance company roof collapse under weight of hailstones in 1990 storm in the western suburbs;

- Australian Stock Exchange flooded in basement computer room;

- Lightening strikes affecting power supply for IBM and other computer users in the Pennant Hills area;

- Newcastle Earthquake;

- Manufacturers Mutual Basement flooded by corroding water pipes.

- Cyclones in Darwin

Motives - slide 17

Motives

There are number of motives for wanting to breach organisation information systems.

Financial gain

© SANS Institute 2000 - 2005 Author retains full rights.

Revenge, Disgruntled Employee

Political

Industrial Espionage

To attack another company

Personal Prestige

For a cracker to say they had broken into a Government* / Financial* / Corporate site*

* Use where applicable to the client.

Targets - slide 18 - 19

Why would organisation be a target?

The organisation is seen as a [eg - *government institution*],

It is involved with minority groups,

> ***NOTE: consult with management to ensure other relevant reasons are included.***

Threats specific the organisation

> ***NOTE: We would consult with departmental management to ensure relevant threats are included.***

Information security documentation - slide 20

The Information Security Policy applies to all organisation information systems not just to those provided by IT. It is a definite course of action adopted as a means to an end expedient from other considerations. The policy does not cover hardware/software specific issues as these are covered in the Information Security Standards and Procedures. The policy contains a statement clearly stating a course of action to be adopted and pursued by organisation and contains the following.

Information security can be seen as balance between commercial reality and risk

- Forward - The information Security Policy contains a forward by the CEO explaining the reason for the Policy.

- Scope - The scope of the document relates to all of organisation Information assets not just those on the main frame.

© SANS Institute 2000 - 2005 Author retains full rights.

- Policy Statement - The policy statement is just that a statement of intent.

- Objectives - The objectives outline the goals for information security. As you can see they are quite extensive and will continue to be added to as new technologies are introduced.

- Statement of Responsibilities - This is an important section as it outlines who is responsible for what, right from the board of directors

Information Security Standards and Guidelines

A standard can be defined as a level of quality, which is regarded as normal adequate or acceptable. The purpose of the information security standards is to define the minimum standards, which should be applied for handling organisation information assets. The standards documentation contains various chapters relating to USERIDs and passwords, emergency access, communications etc.

The information security Standards should be used as a reference manual when dealing with security aspects of information. It contains the minimum levels of security necessary for handling organisation Information Assets.

Information Security Procedures

Procedures can be defined as a particular course or mode of action. The procedures explain the processes required in requesting USERIDs, password handling, and destruction of information.

The Information Security Procedures can be described as the "action manual". It contains the following sections on how to.

- USERIDs Request Procedures - This section outlines in detail the steps required to request access to the system or, change access or suspend/delete access. There are clear easy to follow steps with diagrams of the panels you will encounter and instructions on how to complete the different fields. There are individual sections on good password procedures, reporting breaches of security and how to report them

- Personnel Security Procedures - This section outlines personnel

© SANS Institute 2000 - 2005 Author retains full rights.

security procedures for hiring, induction, termination and other aspects of dealing with information security personnel issues.

- Disposal of Sensitive Waste - The disposal of sensitive waste is indeed a high profile one now especially in light of recent stories in the popular press. It is amusing to see what is on the back of the reused computer paper that comes out of the kindergarten. Dumpster Diving is even depicted by Hollywood!

Frequently Asked Questions

While the policy document and the standards and procedures have in most cases tried to minimise the use of information technology jargon sometimes it is unavoidable. The Frequently Asked Questions Section can be described as the no jargon approach to information security! In essence, it can be described as an encapsulation of this workshop. It is written in an easy to understand question and answer format designed to cover most of your questions, under the following headings:

- Introduction;
- Description Of Information;
- Description Of Information Security;
- Your Role;
- Use of Personal Computers;
- Consequences Of Security Breaches;
- Further Information.

All of this documentation should make your working life considerably easier because you will be able to refer to the documentation rather than seeking advice from your managers' peers or the security group. Obviously if you are unclear of the definition or interpretation, check with you manager or the security team.

Your role in information security - slides 21 - 30

© SANS Institute 2000 - 2005 Author retains full rights.

Why You Should Be Concerned About Information Security

The information you use every day must be protected whether you work with paper records or computer systems. If this information was unavailable or inaccurate, it could cause organisation to lose credibility and you could affect your job. Good security assists in the well-being of the organisation by ensuring the information that you work with is available and accurate.

Why Do We Need Controls?

Controls are required to ensure each person is accountable for his/her actions. Controls protect the innocent from unwarranted suspicion. Without accountability, all are equally suspect when something goes wrong. Problems with information systems are normally caused by honest errors or omissions. Controls help identify quickly those who require help and limit the effects of damage. They also assist in streamlining rather than impeding workflow and can subsequently enhance productivity.

Information is an asset and the loss of this asset can cost time and money. Incorrect information can lead to all kinds of problems. Here are just a few of the things that could result from poor security:

- Information could be lost costing organisation money to recreate it;
- Management could make a bad decision based on incorrect information;
- Giving out private information could cause the organisation embarrassment. As a result organisation may end up in litigation;
- A rival may obtain company information causing organisation to lose competitive advantage.
- Damage to Reputation (eg Bob Carr and $50 cheques to the deceased)[26]

People Are Important Too

The organisation recognises that the employees are IT most important asset.

[26] *The **Sydney Morning Herald** report, "a man from western Sydney was displeased when he received a $50 back-to-school allowance cheque for his son. The cheque, which arrived 15 months after the death of the man's wife, was made out to 'Mrs Passed Away'. The man said his 15-year-old son initially thought the letter, from New South Wales Premier Bob Carr, was a 'sick joke'. On realising it was an official communication, the man said, he decided 'he can keep his lousy $50'. Carr told reporters that 'we apologise unreservedly' but that, as he didn't address the envelope, he was not in a position to offer the family a personal apology. The man replied: 'We do something wrong by the Government and they're into us. As soon as they make a mistake you get a flippant apology."*

© SANS Institute 2000 - 2005 Author retains full rights.

The safety and security of the employees is paramount to the management. The organisation seeks to ensure the security and safety of IT employees by using various security, health and safety programmes. Security whether it is physical or logical is important for both you and the company and the policies and procedures exist to protect both you and the organisation. The role you have to play in the well being of organisation should not be underestimated, as you are the key to IT success.

You can assist in Good Security Practices such as in many ways:

- protecting Information In Your Work Area (clear desk etc);
- password and USERID Controls;
- software Use;
- good Backup Procedures;
- using organisation Computers At Home;
- disposal Of Sensitive Information;
- reporting Problems

Password and USERID Controls

Your password is for your own personal use. You are responsible for access made under your USERID and password.

Password Selection Techniques

Your password can be protected using the following methods:

- Change your password periodically;
- Change your password if you suspect somebody else might know it;
- Choose hard to guess but not hard to remember passwords;
- Enter your password in private;
- Do not use passwords which can easily be associated with you such as

© SANS Institute 2000 - 2005 Author retains full rights.

family names, car and telephone numbers, birth dates etc; your USERID; all the same characters or consecutive characters on a keyboard.

Remote Access

Take care of the laptops, do not use them or leave then on public transport and do not let your children play with them.

Secure Disposal of Information

Some of the methods that may be used are:

- Shred the document. Shred the reports down the page instead of across because reports are very readable if you shred them so the lines of print can still be read! With microfiche feed the documents in at an angle;
- Place the document in a special collection bin for sensitive rubbish,
- If worn out floppy diskettes have sensitive information on them, cut them in half before disposing of them; and
- If a diskette contains sensitive information do not pass it on to anyone else, information still resides on the disk and is retrievable even if it has been reformatted.

Security Breaches

Some breaches such as stealing, wilful damage and breaking statutory regulations are considered criminal offences. Copying of proprietary software is also a criminal offence as has been shown in some well-documented cases where companies and individuals have been taken to court by the BSAA.

- Other breaches of security may not be criminal offences but could embarrass organisation.
- Breaches of security could result in suspension or even dismissal.
- Breaches of security whether they are deliberate or accidental can affect all of us at organisation.

The handling of security breaches is very important and the following points should be considered:

© SANS Institute 2000 - 2005 Author retains full rights.

Responsibility

It is the responsibility of all users to report any suspected breaches of security to the management and ISD. This is of particular importance if you suspect the breach may have occurred under the improper use of your USERID.

Notification

Do not discuss suspected breaches with anyone other than your immediate manager and IT Security and control even though you may be tempted. This is for your own protection. It helps to guard you against any possible recriminations should the suspicion prove to be either proven or unfounded. This point cannot be overemphasised.

Investigation

Do not attempt to solve the problem or pursue any further investigations yourself. This is the responsibility of user management and Internal Audit with assistance from ITS.

Any suspected reported breach will be treated with the utmost confidence and will precede no further if proved unfounded.

Details to be reported

- USERID and owner name, location, section, department of the person reporting the breach.
- Name and USERID of the person suspected of committing the breach
- Details including systems time and possible evidence i.e.: logs, transaction reports etc.
- Outcome or possible outcome of the breach.

Retain any documentation relating to the breach, copy it and forward it to ITS. If possible, the documentation should be delivered in person.

Accidental Breaches

Accidental breaches should be communicated to your immediate management and the security group immediately to relieve any unwarranted suspicion and to save valuable time in tracing the source of the breach.

Secure Handling of Information

It is important that the following documents be handled with care:

- Network diagrams

© SANS Institute 2000 - 2005 Author retains full rights.

- Internal telephone directory
- Organisational charts

There Are Legal Reasons why you should protect organisation Information

There are federal and state laws that make you legally responsible for ensuring information is correct and used appropriately. The laws relate to:

- Protecting a person's right to privacy;
- Inappropriate Data;
- Prohibiting violations of copyrights, patents and trade secrets;
- Prohibiting unauthorised computer access;
- Protecting the privacy of an individual's tax file number.
- Breaching the security and control procedures is a serious matter and cases that are more serious could lead to prosecution.

Operate a Clean Desk Policy

We can become careless about the information in our work area because it is available and we have authorised access to it all the time, but it is important to prevent access by unauthorised visitors. We can do this by following a clean desk policy as described below:

- Documents and keys in a cabinet or drawer;
- Clear desks of all papers at the end of the working day;
- Do not discuss sensitive information in areas where it can be overheard;
- Establish a need to know before discussing information with other workers;
- Label sensitive documents accordingly; and

© SANS Institute 2000 - 2005 Author retains full rights.

- Challenge unauthorised visitors.

Do not read sensitive information on public transport.

- Ensure that anyone you see using a workstation in your area is authorised to do so.

- When sensitive information is on the screen, make sure that no one else can see it. This is especially important when your work area receives members of the public. Make certain that your screen faces away from them.

- Lock the terminal when you leave it even if it is only for a short period.

Use Caution When Handling Visitors

Anyone not currently working in your department is a visitor. Use caution when disclosing information in front of any visitor. This includes:

- Former employees of the organisation;

- Sales people and the organisation clients.

- refer any questions form the media (reporters) to the appropriate people in organisation;

- when asked to complete a survey or questionnaire ask your supervisor first if it is all right;

- If you receive phone calls from vendors or employment agencies, take the individual's name and number and pass this on to the appropriate people. Do not give these people a copy of organisation telephone book. This would allow them to make calls, which others in organisation may not welcome.

- When speaking on the telephone, you could easily be fooled into thinking you are talking to an individual with a real need for some facts. Be careful

© SANS Institute 2000 - 2005 Author retains full rights.

not to give out valuable information to the wrong person. Here are some points to remember:

- Verify the identity of the caller. If you cannot do this by asking some key questions, obtain their phone number and tell them you will call back. Refer the matter to your supervisor or manager.
- Verify the caller's need to know the requested information. If in doubt, check BEFORE giving anything over the phone;
- Be careful not to give out unnecessary information;
- Be aware of who is in the area that could overhear your conversation.

Software Use

Proprietary Software

Any software you write belongs to the organisation if:

- You use company equipment to develop it;
- You develop it on behalf of organisation;
- You develop it on the organisation's time regardless of the equipment you used.

Software written and developed by other employees may only be used if authorised by the owning manager.

Software which has been developed by organisation may not, unless authorised be used by outsiders. This software is organisation intellectual property and has a tangible value especially if organisation decides to market the software.

'Borrowing' Software

Taking copies of software depends on the license agreement with the vendor. It is best to be safe and not take a copy unless your management has permitted it in writing. Misuse of software in relation to copyrighting is a criminal offence with heavy fines imposed for anyone caught copying copyrighted software.

If in doubt, do not copy.

© SANS Institute 2000 - 2005 Author retains full rights.

- obtain your managers approval before copying software;
- although organisation may have purchased the software it will probably be licensed for use on one machine only;
- Unauthorised copying of software is a criminal offence. It is critical for your own protection as well as organisation that you check the terms of the license to ensure you are not violating the agreement with the vendor;
- Some agreements with software vendors may allow the copying of software if the intended use is for business purposes. Check with your manager or LAN support group to see if this applies;
- you may need to register your use of the software with the vendor;
- If you are borrowing an original CD, make a backup copy and use great care in protecting the CD from damage. Only use original CD's in exceptional circumstances and with written approval.

Using the organisation's Computers At Home

This is not recommended as a common practice. Personal computers may be stolen or damaged when they are removed from the office. If you have to take a computer home or are required to carry it with as part of your work practices the following steps must be followed:

- Obtain written approval from your manager;
- Use extra care in handling the equipment, as it is very fragile.

The same rules apply both at work and at home. Make sure you know the classification of the information and that the appropriate controls are applied. Be sure to:

- Store the computer and storage media in an appropriate environment. I.e. away from heat and damp, etc.
- lock up the information when not in use;

© SANS Institute 2000 - 2005 Author retains full rights.

- Ensure that all files are encrypted according to the Data protection policy standards;
- make backup copies and protect them the same as the originals;
- protect the information from damage;
- protect the information from observance by unauthorised individuals;
- Do not allow the computer to be used for any other purpose than work.

Bringing Your Own Home Computer to the Office

This is not permitted for the following reasons:

- The organisation's insurance policy does not cover the equipment if stolen;
- If it is stolen organisation will not replace it.
- The possible introduction of a Computer Virus etc

Reporting Problems

Full details to the Help Desk

The 10 Commandments of IT Security – Slides 31 - 32

The following is a code of ethics suggested by the Computer Ethics Institute, Washington, DC, USA.

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

7. Thou shalt not use other people's computer resources without authorisation or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the programme that you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that insure consideration and respect for your fellow human being.

The future of security – Slide - 33

1. The area of information security will not diminish in IT complexity; in fact, it will become increasingly complicated with the further strengthening of privacy legislation and business resumption insurance requirements.

2. There are a number of interesting developments taking place in technology. Some of these may have already affected the way in which you conduct your work. Technological developments will occur that most certainly will change your role sometime in the future. Some of these can be described as follows:

Identification Techniques

Current identification techniques rely mainly on passwords and USERIDs to verify a person's access. Passwords however are **not** the most secure method of identification as someone can see you typing them in or can take an educated guess at them. With the number of systems we have to access with a USERID and password or PIN numbers, the temptation to write them down can be very seductive. There are moves to use other means of identification that require you to remember nothing - except yourself! Biometrics traditionally developed from identification techniques in science fiction movies and for the military. Now they are now gaining acceptance within the commercial environment. Finger scanning is already in use in some government departments, financial institutions and in private industry. Finger scans can be used to identify you are as a control technique for online authorisations of cash payments etc. Finger scans have wide acceptance with unions as they protect the innocent from unwarranted suspicion and deter the "would be" fraudster. The surface of the fingerprint is stored as digitised signature and not a fingerprint. The recognition device only works on live fingers, not on dead fingers, photocopies or rubber fingers[27]!

© SANS Institute 2000 - 2005 Author retains full rights.

Summary –Slide 34

The information technology area of recent years has been one of rapid change and the dependence of the business function on information processing has increased the vulnerability to threats. As discussed, threats can take many forms. These range from sabotage, fraud and in the majority of cases and the largest dollar loss human errors, accidents and omissions. Security processes are no longer restricted to physical locations and a computer crime is more likely to take place through communications networks.

The area of information security will not diminish in complexity; in fact, it will become increasingly complicated with the further strengthening of privacy legislation and business resumption insurance requirements. Other issues such as Imaging Systems, Executive Information Systems and Quality Accreditation all add to the complexity.

It is not enough to develop the policies, standards and procedures line management assume responsibility for enforcing the security policies and taking a pro-active approach.

Without the availability confidentiality and integrity of information, the ability of organisation to provide the efficient reliable and quality services to IT customers, business partners and employees diminishes. The need arises for a coordinated approach in designing and implementing a security programme that will provide flexible cost effective solutions while still protecting organisation information assets and allowing the employees to perform their duties in a secure and safe environment without any unnecessary barriers.

It is a salient point that sharing information increases it in value both within the organisation and outside of it. This is true whether the information sharing occurs with friendly or hostile parties.

Where to get more information – No slide at present – 35

This will depend on organisational requirements.

[27] Contrary of what Hollywood tries to tell us, modern biometric devices do not work on dead tissue or plastic.

© SANS Institute 2000 - 2005 Author retains full rights.

Appendix C, Sample Managerial assessment interview questionnaire

	Question	Answer
1	Is a current information security awareness programme in place to ensure all individuals who use information technology resources or have access to these resources are aware of their security responsibilities and how to fulfil them?	
2	Is the programme approved by the ISSO?	
3	Does the process specify timeframes and re-training requirements?	
4	Is it fully documented?	
5	Are new employees trained within 30 days of being hired?	
6	Do all employees sign that they have understood and accept the training and organisational policies?	
7	How often is refresher training provided?	
8	Does your staff know what's expected of them in their role regarding security for the organisation, and your division?	
9	When did you last attend a security workshop for staff provided by the Security Division?	
10	Is our contract is included in security awareness sessions?	
11	What areas do the awareness training cover (eg password practices, use of anti-malware)?	

© SANS

© SANS Institute 2000 - 2005 Author retains full rights.

Computer Security Awareness – Example Quiz copied from the Fermi National Accelerator Laboratory[28]

All lab employees and visitors are asked to take a few minutes today to complete the following simple computer security awareness checklist. This will help ensure that they understand some basic principles and are following proper computer security practices. (We'll help you out you with one small hint: the correct answer to questions 1 through 8 is YES.) More detailed information about particular topics will follow in subsequent articles; some additional information about each question can be seen by following the web links.

Computer Security Awareness checklist:

1. ***Passwords***
   Are all of your accounts protected by distinct strong secure passwords that are not written down or shared with others?
   YES ___ NO ___
   Tell me more

2. ***Unattended machines***
   When your desktop machine is left on in an unsecured area (such as an unlocked office) is it protected with a password-based screen saver (and physically secured as well)?
   YES ___ NO ___
   Tell me more

3. ***Local system administration and registration***
   Do you know exactly who is responsible for system administration of the machine on your desktop, and in particular for installing new security patches and maintaining a secure configuration? (This could be yourself.)
   YES ___ NO ___
   Has that local system administrator (perhaps yourself) registered your machine and his/her identity in the lab's computing equipment database (so that he/she can be quickly notified of urgent computer security issues concerning your machine)?
   YES ___ NO ___
   Tell me more

[28] http://computing.fnal.gov/security/checklist.html

© SANS Institute 2000 - 2005 Author retains full rights.

4. ***Data backup***
   Are you aware of the procedures used to create backup copies of any data that you are responsible for, and have you ever tested these procedures by retrieving backed up data?
   YES ___ NO ___
   Tell me more

5. ***Reporting suspected computer security incidents***
   Do you know how to report a suspected computer security incident?
   YES ___ NO ___
   Tell me more

6. ***Virus protection***
   Is virus protection software running, with up to date virus signatures, on all Windows PCs that you use?
   YES ___ NO ___
   Tell me more

7. ***Safe email practices***
   Do you exercise extreme care in dealing with email, in particular almost never opening attachments unless you are absolutely certain of their origin?
   YES ___ NO ___
   Tell me more

8. ***Safe web browsing***
   Do you exercise extreme care in browsing the web, in particular using safer and patched browsers (Internet Explorer is specifically not recommended for general use), turning off ActiveX, and being cautious in clicking on new links?
   YES ___ NO ___
   Tell me more

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Example - Security Awareness Evaluation Form[29]

Location: _____ Class Date _____

Instructor _____

Your evaluation and comments will help us ensure this class is continuously improved to meet our security needs and requirements. Thank you for your support.

Please answer the questions using the following key:

1 = Strongly Agree 2 = Agree 3 = Disagree 4 = Strongly Disagree 5 = Not Applicable

1. The purpose of this course was clearly communicated.	1 2 3 4 5
2. I found value in the information presented.	1 2 3 4 5
3. The instructor(s) were responsive to questions and informative.	1 2 3 4 5
4. The instructor(s) were clear in their presentations.	1 2 3 4 5
5. The classroom was comfortable.	1 2 3 4 5
6. I could see the presentation clearly.	1 2 3 4 5
7. I could hear the presentation clearly.	1 2 3 4 5
8. I received enough information prior to the class to be prepared.	1 2 3 4 5
9. My overall impression of the instructor(s): Comments:	___ Excellent ___ Good ___ Fair ___ Needs Improvement
10. My overall impression of the facilities: Comments:	___ Excellent ___ Good ___ Fair ___ Needs Improvement
11. My overall impression of the course: Comments:	___ Excellent ___ Good ___ Fair ___ Needs Improvement

[29] © Copyright 2002. Melissa Guenther, LLC. All rights reserved.

© SANS Institute 2000 - 2005 Author retains full rights.

Do you have any additional comments you believe will help improve the class for others in the future?

Your name, office designator, and phone number if you would like to be contacted: **Thank you very much for your cooperation.**

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Appendix D, Sample awareness materials

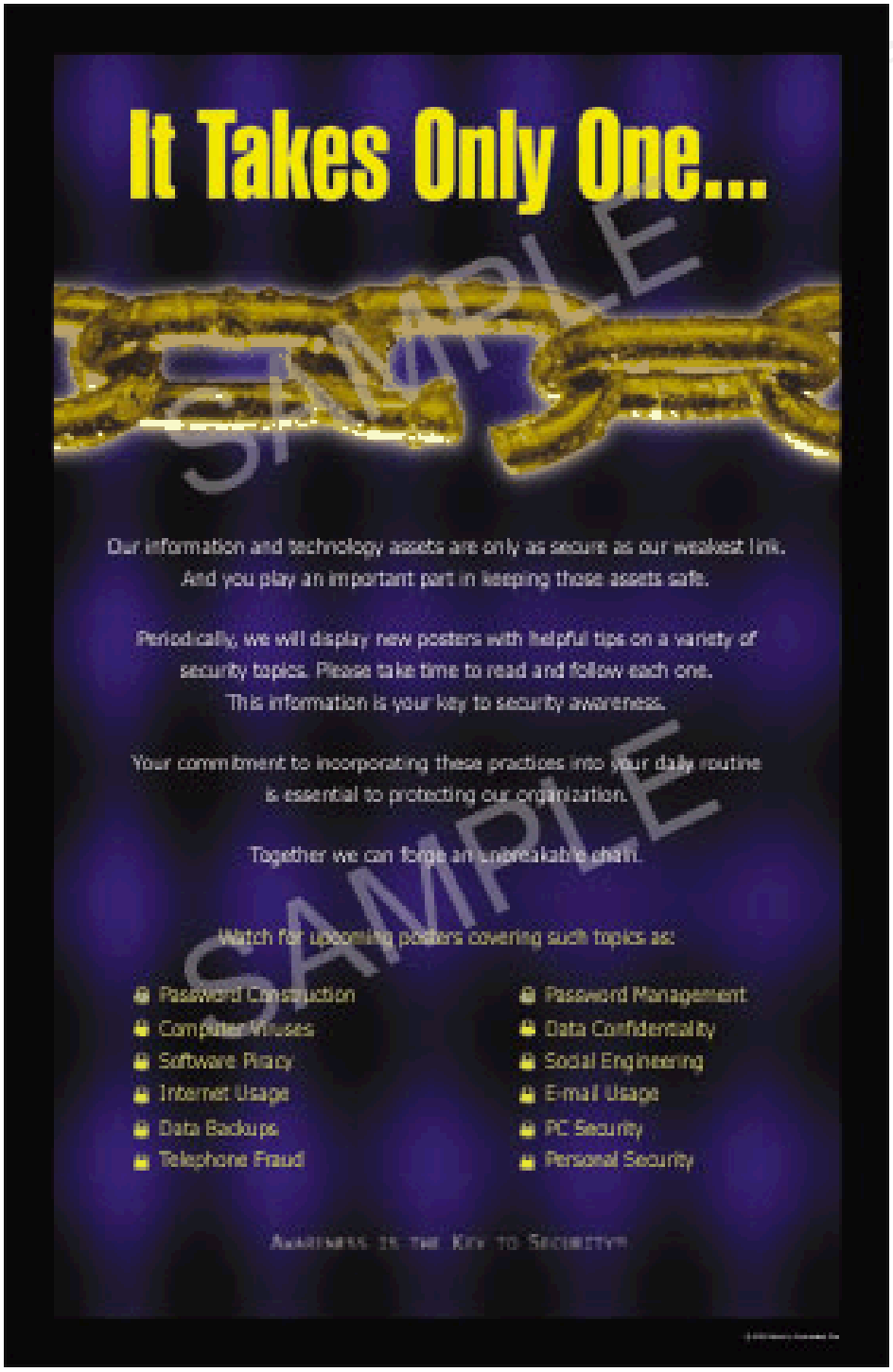


Figure 4 - Sample awareness materials 1

http://www.securityawareness.com/introducs.htm

© SANS Institute 2000 - 2005 Author retains full rights.

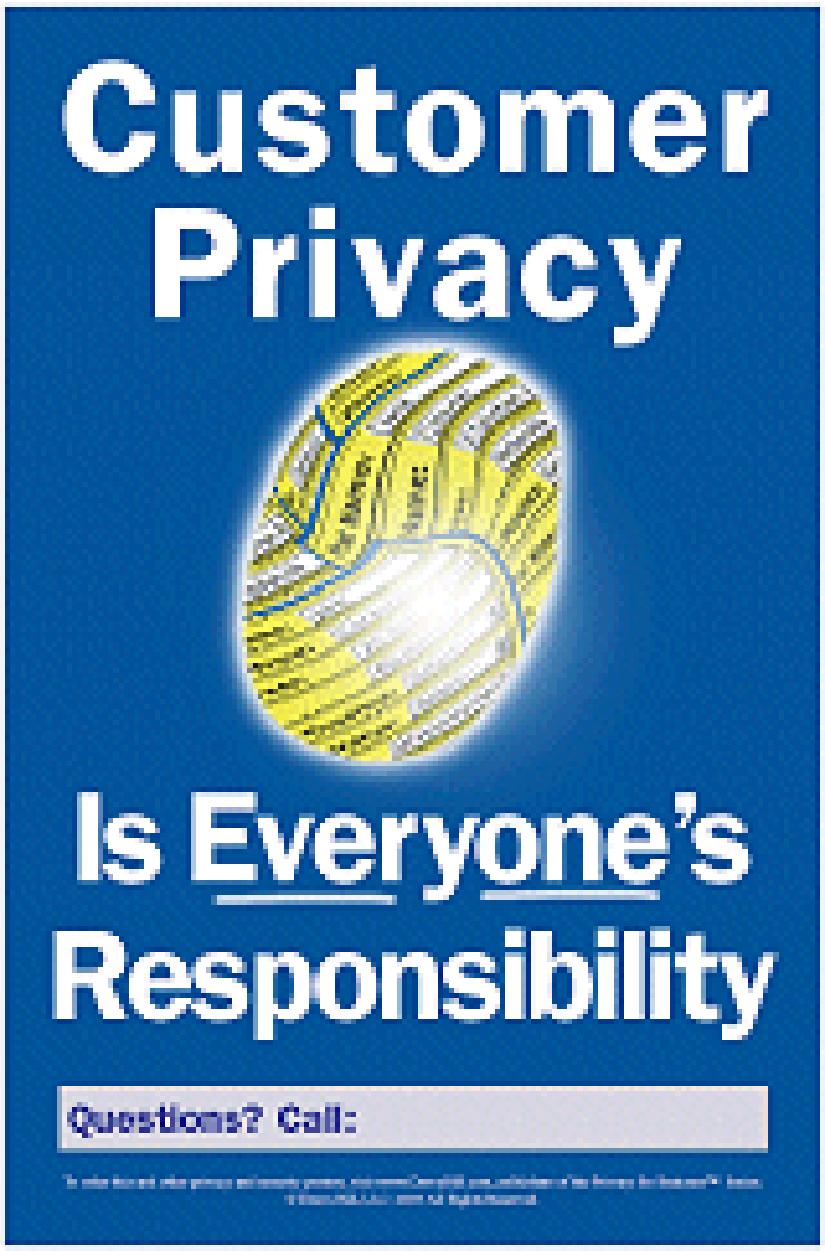


Figure 5 - Sample awareness materials 2

http://www.privacyforbusiness.com/posters.htm

© SANS Institute 2000 - 2005 Author retains full rights.



Figure 6 - Sample awareness materials 3

http://www.noticebored.com/NB_poster_Think_dont_link_3_SAMPLE.jpg

© SANS Institute 2000 - 2005 Author retains full rights.

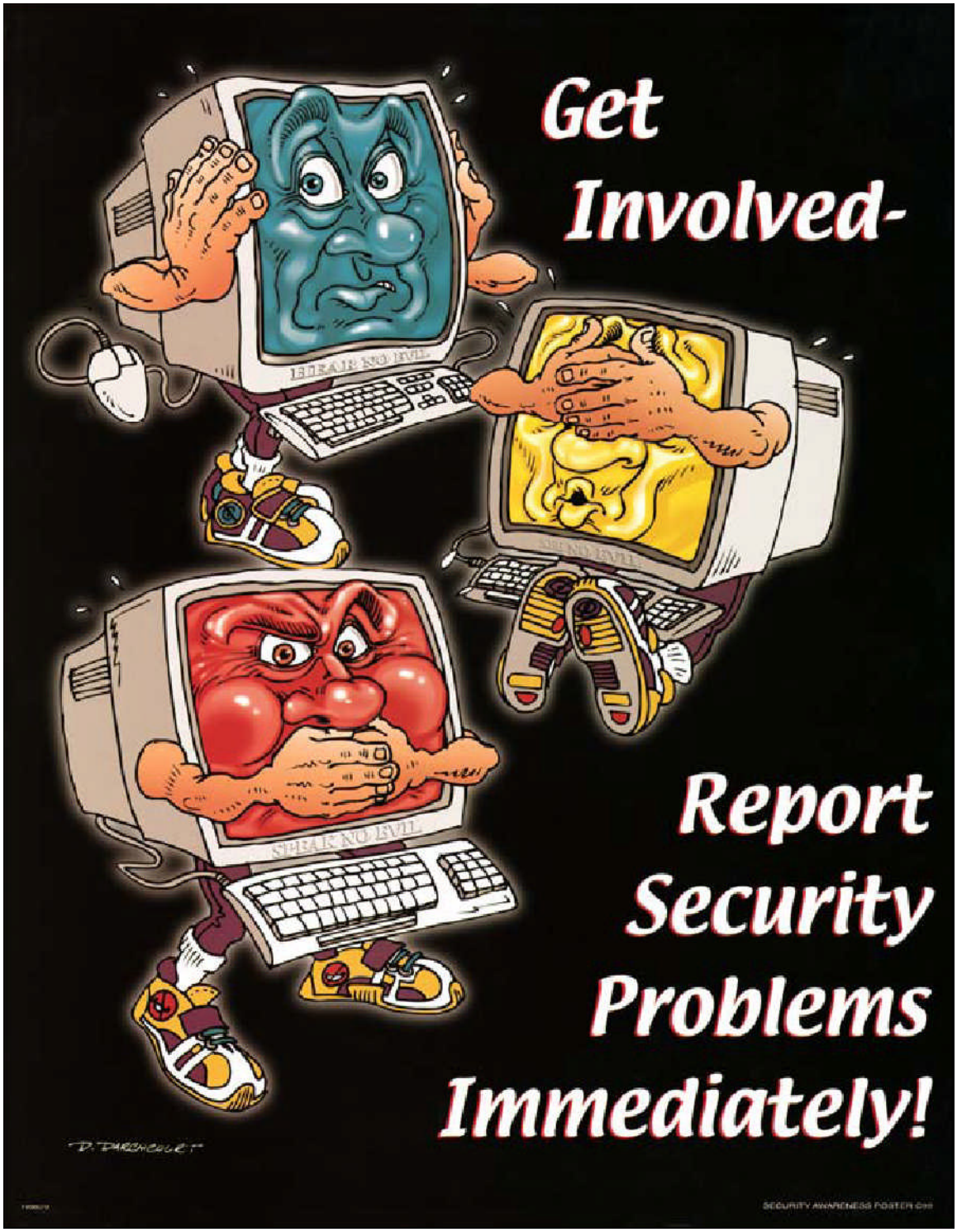


Figure 7 - Sample awareness materials 4

NIST Special Publication 800-50

© SANS Institute 2000 - 2005 Author retains full rights.

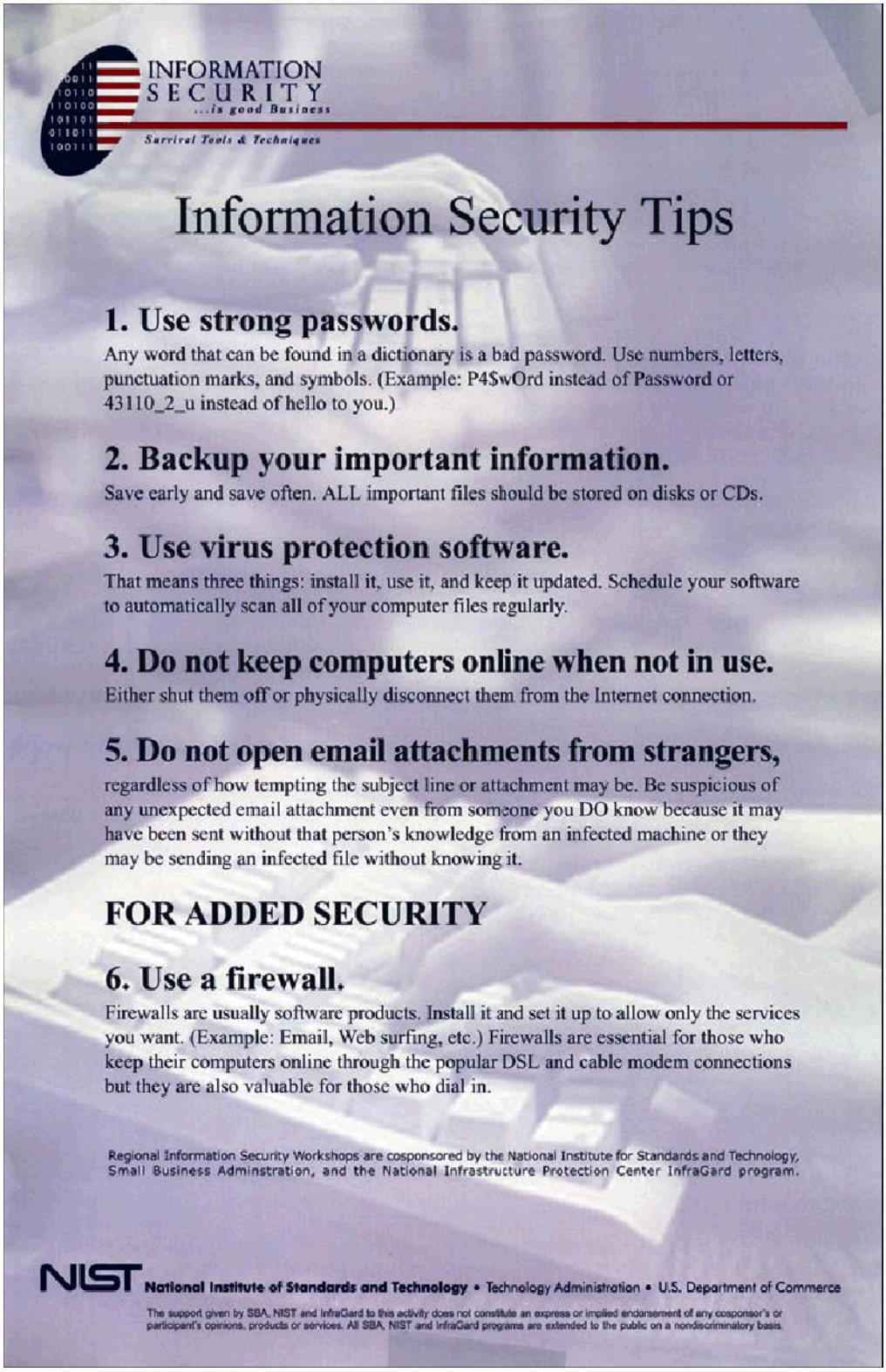


Figure 8 - Sample awareness materials (NIST)

© SANS Institute 2000 - 2005 Author retains full rights.

Appendix E, awareness and training metrics

Sample Human Resources Checklists

HR

1. Do you have systems and procedures to ensure that the staff are kept adequately aware of the organisations security policy and processes?
2. Has the organisation implemented policies and procedures to address security incidents, and a contingency plan to respond to emergencies?
3. Has the staff been tested recently to assess their levels of knowledge of the contingency plan etc?
4. Do you have systems and procedures to ensure that security staff are adequately trained?
5. For assets that are vulnerable to internal risks, has the organisation clearly laid out access level permissions for the employees using the critical processes?
6. Are staff induction processes operating correctly? Have post-induction tests been completed for a sample of the staff?
7. What processes are used to test the staff?
8. How often are the staff "reminded" of their security obligations?

Internal Process Assessment

1. Have you assigned security responsibilities in your organisation?
2. Have you established personnel clearance procedures, including context-based access, user-based access and role based access?
3. Do you maintain a record of signed access authorisation?

© SANS Institute 2000 - 2005 Author retains full rights.

4. Do you have a schedule for employee training for security technology and procedures?

5. Do you conduct employee background checks?

Reporting Procedures' Assessment

1. Has the Information Security policy been communicated to all employees and contractors?

2. Are the board of directors and Senior Management involved in the security process?

3. Do you have reporting procedures and forms for reporting all intrusions, attempted intrusions and the status of security infrastructure to the board of directors?

4. Do these reporting procedures include forms for communication and updating staff access (for example departing staff or staff transferring to another department)?

Appendix F, Training Programme Planning Template

As modified from NIST Special Publication 800-50

Executive Summary

A few simple paragraphs summarising the objectives of plan.

Background

What policies and controls are the driving factors in the development of this training/awareness programme and plan?

Relevant IT security policy

- Goals
- Objectives
- Roles and responsibilities

© SANS Institute 2000 - 2005 Author retains full rights.

Awareness

- Audience (eg staff group or management)
- Activities and target dates
- Schedule
- Review of materials and methodology

© SANS Institute 2000 - 2005, Author retains t

© SANS Institute 2000 - 2005 Author retains full rights.

Training/Education

Role one:

Executives and Management

- Learning objectives
- Focus areas.
- Methodology and activities
- Schedule
- Credential evaluation criteria

Role Two:

General IT Staff

- Learning objectives
- Focus areas.
- Methodology and activities
- Schedule
- Credential evaluation criteria

Role Three:

Information security professionals

- Learning objectives
- Focus areas.
- Methodology and activities
- Schedule
- Credential evaluation criteria

Network administrators and engineers

- Learning objectives
- Focus areas.
- Methodology and activities
- Schedule
- Credential evaluation criteria

© SANS Institu ıs full rights.

Professional certification

Role one:

General IT Staff

- Learning objectives
- Focus areas.
- Methodology and activities
- Schedule
- Credential evaluation criteria

Role Two:

Information security professionals

- Learning objectives
- Focus areas.
- Methodology and activities
- Schedule
- Credential evaluation criteria

Role Three:

Network administrators and engineers

- Learning objectives
- Focus areas.
- Methodology and activities
- Schedule
- Credential evaluation criteria

Include other roles as required.

© SANS Institute 2000 - 2005 Author retains full rights.

Resource requirements and funding

Cost

- Staff costs
- External contractors
- The facilities[30]
- Training media[31]

$ xxx.xx

$ xxx.xx

$ xxx.xx

$ xxx.xx

© SANS Institute 2000 - 2005

[30] The facilities include training rooms, conferencing and other facilities.

[31] Training media includes computer-based training materials, Web-based systems, handouts, etc.

© SANS Institute 2000 - 2005 Author retains full rights.

Bibliography

Organisational References

1. Administrative committee on coordination, Information Systems coordination committee (ISCC), “Information security: recommended practices for United Nations organisations”, 1994.
2. “Computer Security Awareness Training and the Interactive Learning Framework”, By McDonald Bradley, Inc. January 10, 2002
3. “EDUCATION AND TRAINING”, Guidance Notes on the application of ISO 9001 for quality management systems in Education and Training, BSI, Revised 1999.
4. “HOMELAND SECURITY”, HEARINGS before the COMMITTEE ON APPROPRIATIONS UNITED STATES SENATE ONE HUNDRED SEVENTH CONGRESS SECOND SESSION, SPECIAL HEARINGS, APRIL 10, 2002--WASHINGTON, DC, APRIL 11, 2002--WASHINGTON, DC
5. FISSEA 2003 Annual Conference: "Securing Your Cyber Frontier Through Awareness, Training and Education" Agenda and Presentations - March 4-6
6. Information Security Management, Part2: Specification for Information security management systems AS/NZS 7799.2:2003 BS 7799.2:2002
7. Information Technology – Code of practice for Information Security Management AS/NZS ISO/IEC 17799:2001
8. ISACA, (2003) CISA REVIEW MANUAL, ISBN: 1-893209-42-3
9. NIST Special Publication 800-12, “An Introduction to Computer Security: The NIST Handbook”.
10. NIST Special Publication 800-16, “A Model for Building Training Courses”.
11. NIST Special Publication 800-26, “Security Self-Assessment Guide for Information Technology Systems”.
12. NIST Special Publication 800-30, “Risk Management Guide for Information Technology Systems”.
13. NIST Special Publication 800-35, “Guide to Information Technology Security Services”.
14. NIST Special Publication 800-47, “Security Guide for Interconnecting Information Technology Systems”.
15. NIST Special Publication 800-50, “Building an Information Technology Security Awareness and Training Programme”.

© SANS Institute 2000 - 2005 Author retains full rights.

16. NIST Special Publication 800-61, “Computer Security Incident Handling Guide”.
17. NIST Special Publication 800-64, “Security Considerations in the Information System Development Life Cycle”.
18. NIST FIPS PUB 201, “Personal Identity Verification (PIV) for Federal Employees and Contractors PUBLIC DRAFT”.
19. SANS Institute, The. “Risk Management.” Kickstart Track Book KS-1A/B (2001), Chapter 1, pp 1-23
20. SANS Institute, The. “GIAC Basic Security Policy.” Track 1: Security Essentials Book 1.1, Version 1.4 (2001)
21. SANS Institute, The. “GIAC 7799.” Track 4: ISO 17799 Book 1.1, (2005)
22. SANS Institute, The. “Information Security Management System (7799) for an Internet Gateway.” Amarottam Shrestha, G7799 Practical Assignment, (2004)

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Published References

23. Cooper, Lynne P., Nash, L. Rebecca, Phan, Tu-Anh T., Bailey, Teresa R., (2004), "Using Knowledge-Based Systems to Support Learning of Organizational Knowledge: A Case Study", Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA 91109-8099.
24. D. Pottas , Sebastiaan H. von Solms, Superseding Manual Generation of Access Control Specification - From Policies to Profiles, Proceedings of the IFIP TC11, Ninth International Conference on Information Security: Computer Security, p.327-342, May 12-14, 1993
25. Guenther, Melissa, (2002) "Security Awareness Evaluation Form" Melissa Guenther, LLC.
26. Hannagan, Tim, 2002, '*Management, Concepts and Practices'*, 3rd Edn, Pearson Education Ltd, UK,
27. Katzke, S, "A Government Perspective on Risk Management of Automated Information Systems", Proc. 1988 Computer Security Risk Management Model Builders' Workshop, NBS, Gaithersburg MD, USA, 1988.
28. Kindon, John W. (1984), "Agendas, Alternatives and Public Polices", Boston, Little, Brown.
29. Mead, Richard, 1998, '*International Management, Cross-Cultural Dimensions'*, 2nd Edn, Blackwell Publishing, UK,
30. O'Brien, James A., 1999, '*Management Information Systems, Managing Information Technology in the Internetworked Enterprise'*, 4th Edn, Irwin McGraw-Hill Ltd, US.
31. Oud, Ernst J. "ISO/IEC 17799 Compliance", "COBIT Security BaselineTM and ISO/IEC 17799 compared", and "Using COBIT for BS 7799-2 compliance audits"
32. Ozmen, Kemal "IT Risks and Controls: Risk Identification, Risk Mitigation, Risk Management, Controls Implementation"
33. Ruthberg, Della G. Tipton, Harold (1993), "Handbook of Information Security Management"
34. Taylor, G.J., Parker, J.D.A., and Bagby, R.M. (1999). "Emotional intelligence and the emotional brain: Points of convergence and implications for psychoanalysis". Journal of the American Academy of Psychoanalysis, 27(3), 339-354.
35. Wood, Charles Cresson, (1999) "Information Security Policies Made Easy – Version 7".

© SANS Institute 2000 - 2005 Author retains full rights.

Web Sites

36. Abby, Christopher, "The human firewall", 28/10/2003
http://cio.co.nz/cio.nsf/0/CD50373FD1A06BD3CC256DCD00015C68?OpenDocument

37. Hay/McBer (2000). "Research into teacher effectiveness: A model of teacher effectiveness report by Hay McBer to the Department for Education and Employment". Report prepared by Hay/McBer for the government of the United Kingdom,
http://www.dfee.gov.uk/teachingreforms/mcber/.

38. McCarthy , John, "RISK MANAGEMENT, Plan for People, Not Just Systems "
http://www.cio.com/archive/111501/where.html

39. McLelland, Ross (2004), "emotional intelligence in the Australian context", Pacific Consulting,
http://www.pacificconsulting.com.au/articles_ei.htm

40. Thiagarajan, Valliappan, (2003), "ISO 17799 CHECKLIST" SANS Institute,
http://www.sans.org/score/checklists/ISO_17799_checklist.doc

41. Computer Security Awareness –Quiz from the Fermi National Accelerator Laboratory,
http://computing.fnal.gov/security/checklist.html

42. Countering financial crime risks in information security [Financial Crime Sector Report]
http://www.fsa.gov.uk/pubs/other/fcrime_sector.pdf

43. "Implementing BS7799: A Blueprint", (2004)
http://www.iso17799world.com

44. TechTarget, (2002) "SECURITY STANDARDS: STANDARD PRACTICE"

© SANS Institute 2000 - 2005 Author retains full rights.

http://infosecuritymag.techtarget.com/2002/mar/iso17799.shtml

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.