Chapter 10

Assessing Security Awareness and Knowledge of Policy

This chapter includes:

The creation of an awareness program.

Testing Knowledge and Security Awareness

Introduction

In this chapter we look at what is needed to ensure the success of a security program, awareness. This process, as defined in the NIST[1] 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 program.

It is crucial that the senior management and executives of an organization lead by example. All users within the organization must be aware of the need for security and of their responsibilities in order that for any security program 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 organization. Security awareness allows people to understand their role within the organization from an information security perspective. Awareness helps people realize the need for further training and education.

In planning the development of awareness, training and education programs 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 behavior from an information security perspective. Awareness sessions allow users to become knowledgeable in their responsibilities as they are taught correct practice within the organization. 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 organization's information security assets has been implemented.

[1] 4 NIST (National Institute of Standards and Technology) Special Publication 800-50

No staff member may be expected to conform to the organization'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 organization. Security awareness program help users understand their responsibilities, and allow the users to address the need for a security within their role.

Awareness starts as the first stage of an information security awareness, training, and education program. 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 program. Awareness is a continuing process to alter the user's behavior and attitudes.

Security Awareness and Training

Organizations 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.

In most organizations, the education required 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.

User awareness of security-related issues is becoming an essential component of an effective security program. In the nineteen seventies and eighties, centralized administration did not require as much training and communication for the end user community. Security issues were mostly addressed by MIS and security personnel. From the nineties on however, with the proliferation of client/server applications and decentralized data, it has become increasingly more important that a good and effective security awareness program be part of an overall security implementation.

Security awareness training is required to emphasis the need for security and effective controls in the development and use of information systems. Users of these systems must be educated in the positive benefits of information security and the fact that security measures can actually save time and money by reducing the numbers of errors and accidents which form the bulk of threats to information systems. The additional benefit of security awareness training is the introduction of the 'ethos' of good practice and will flow on into other areas of your organization. A greater understanding of information systems, how to use them and how to gain access to them will reduce the overhead on support services.

For any information security awareness and training program to be successful, detailed planning is essential. The planning of awareness and training programs must consider the whole life cycle from the beginning of the process to completion. The following seven steps as developed in the NIST CSAT[2] program may serve as a starting pointing the development of the program:

1. the programs Scope, Goals, and Objectives need to be identified;
2. the program trainers need to be selected;

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

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

The process requires the completion of the following tasks:

1. Establishing the organizational culture (and the associated risk environment);
2. Identifying the organization's risks;
3. Analyzing 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.

The key risks associated with the training and awareness process 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 organization
4. Awareness sessions are not adequately focused on the policies procedures and standards of the organization;
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 program.

Failure to mitigate the risk associated with poor awareness and training techniques increases the likelihood and exposure to other risks within the organization. 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 organization's information security strategy requires all personnel to have sufficient knowledge of the awareness requirements of the organization and that key personnel maintain key competencies in their areas of the ISMS.

To achieve this is necessary to:

1. Determine the necessary competencies within the organization,
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 organization.

Awareness Programmes need to be implemented

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

1. An organization's personnel cannot 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 organization's spending on both information security as well as in computing infrastructure in general.

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

1 Scope, Goals, and Objectives

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

Goals are set for all stages of the program. There should be goals for security awareness, security training, education, and maybe even certification within the organization. ISO 17799 (and hence ISO 2700x) has a mandatory requirement for periodic training in information security awareness. The scope and goals of this program, and thus the objectives need to take into account this mandate.

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

The primary objective of this program is to create and then maintain an appropriate level of protection for all the information resources within the organization by the dissemination of information to all corners of the organization. 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.

Training requirements for the implementation of any security program within an organization include the development of an information security awareness program as well as training and education programs. The scope of this process encompasses all staff within the organization with access to IT information assets. This ranges from employees up to executive management and all levels in between.

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

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

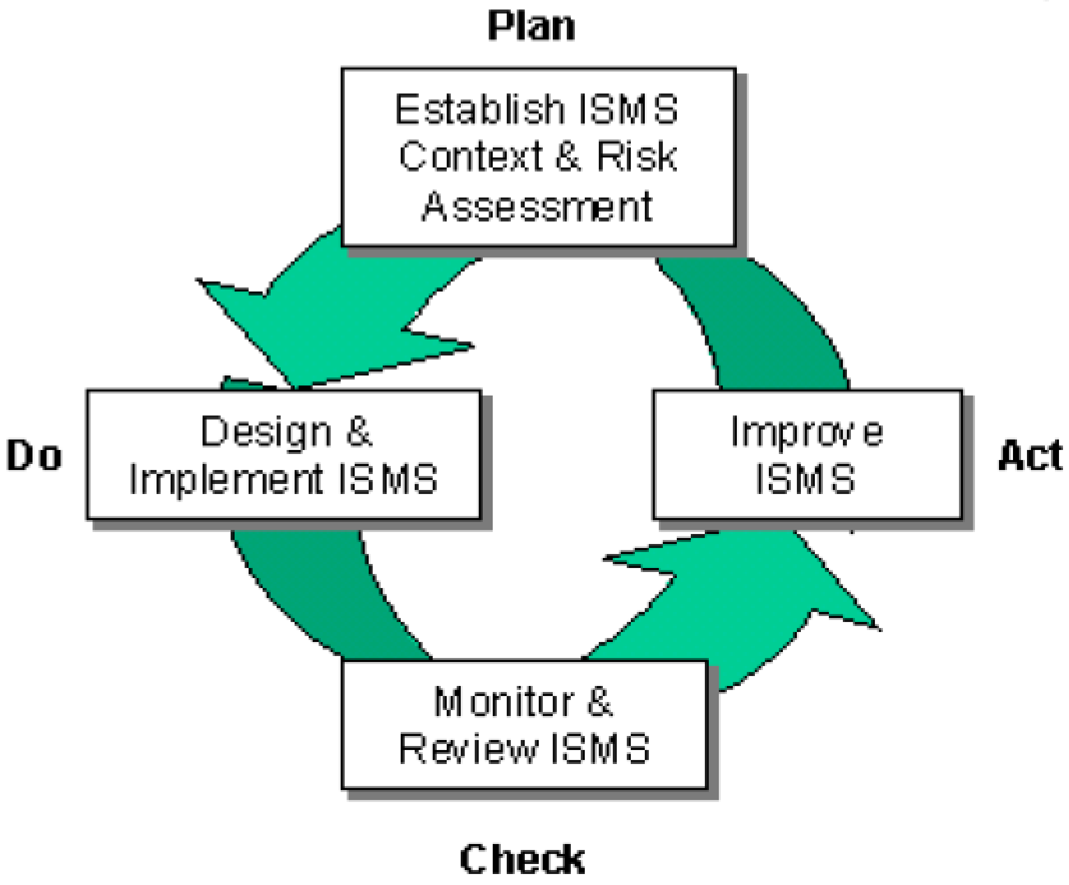


Figure 1 - Plan Do Check Act (PDCA) process

2 Resources

It is essential that the stakeholders in the development of an ISMS awareness training regime should include key representatives of the organization 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 are well versed in information security techniques and principles and have detailed knowledge of the organization'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 organization. Any program that does not consider the costs and availability of resources will not succeed. The creation of an awareness program involves more than just training.

Resources need to be allocated (either within the organization 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 organization, 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 organization, advanced training and even certification may be not only be unnecessary to the organization when applied to all users, but may be detrimental.

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

Training and education programs are best segmented based on the role of the individual within the organization. The users may be segmented into groups such as users, system administrators, management or other relevant organizational 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 program evangelists, key management need to understand how these programs will benefit the organization. Motivating management and executives relies on creating awareness of the need for information security training programs and the risks associated with not implementing these programs adequately.

To further motivate the employees within the organization and to ensure that management not only accept but embrace the program, 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 organization’s security. HR needs to implement disciplinary processes for breaches of the security process and standards within the organization.

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

Individual employees of the organization 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 program actively, they are likely to be both more aware of the requirements for information security and more likely to support the program.

5 Development and implementation of the program

Covered further in the DO stage, development involves the creation of the program. Research needs to be done continuously in order to determine the training needs of the organization. Users must be made aware of –

- The continuing importance of security to the organization,
- 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 organization.

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 programs are highly visible within the organization and the training methods are selected and presented based on the needs of the individual organizational demographics needs.

It is easily seen that the design considerations used for the development of the awareness and training programs must be carefully structured to account for the various levels of knowledge and exposure across the organization’s personnel. Taylor[3] (1999) demonstrated that people exhibit differing modes of learning.

As such, sessions need to be tailored towards individual focus groups within the organization. Emotional intelligenceis an important guide when deciding on teaching skills. The facilitator in an awareness session needs

[3] 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.

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 programs. Additionally, presentations and refresher courses need to be taught separately. On the job and mentoring programs are cost-effective methods of implementing training within several roles.

Security awareness is not a comprehensive information security and training program 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 organizations, training materials may be shared at a lower cost to both organizations. Other organizations with similar needs should be approached for this purpose.

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

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

Awareness should consist of a series of short-term reminders distributed throughout the year, in order to “jog the memory”, making staff aware of their 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 organization’s information security stance.

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

6 Regular maintenance

The rate of change of technology within the information fields drives the need to update any awareness and training program constantly. Awareness training programs 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 organization’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 program requires a high standard of maintenance because of the visibility of this program both internally and externally to the organization. It must also face the current issues of information security affecting the organization. A failure to do this is likely to result in the weakening of the program as staff discount IT usefulness.

7 Periodic evaluations

Program evaluations will be covered in detail later in the chapter. The ISMS (Information Security Management System) ACT stage covers this in detail. It is important to remember that this program 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 programs:

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

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

Awareness

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

It needs to be a condition of employment that all staff read and understands the information policy procedures and standards as they relate to their role within the organization. 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 organization.

It must be made 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 organization. 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 need to 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 organizational need. All existing employees who did not attend awareness sessions when they initially joined the organization 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 organization's overall awareness of information security practices.

Whenever information security policy, procedures or standards change or are 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 organization's policies. The successful completion of an information security and awareness and training program upon employment is a requirement to be granted access to the computer of systems and network.

Education and Professional Development

Any organization needs to recognize 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 organization as part of the employee's career development program needs to work with the employee to ensure their growth and knowledge through specialized 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 hours must be written into their employment contract.

Objectives of an Awareness Program

The main purpose of an awareness program is to inform users about the importance of the information they handle from day to day. It is important that the awareness program inform the users of the business and legal reasons for protecting the integrity, availability and confidentiality of data they possess. Users must be made aware of their responsibilities and the steps the company is willing to take to ensure security.

What Is Information Security Awareness Training?

Security awareness training is a training program aimed at heightening security awareness within the organization. Simply stated, effective security awareness training program should result in:

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

A security awareness program should be an ongoing program 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.

Training description and scope

The introduction of security awareness training 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 while providing a greater sense of shared accountability for the security of the organization's information assets;
- Provide additional benefits 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 between departments.

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 program if required

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

Time Scales

Given that classes should not be greater than 10 – 20 to allow for communication, and that each session should take no more than 2 – 3 hours, the entire staff of most organizations could be covered in a number of weeks (depending on size) using a system of rolling lectures.

Security Awareness Resource Requirements

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

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.

Detailed trainer guide for conducting the 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 organization.

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

Definition of Workshop

The central and most important aspect of this program 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.

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 monopolize 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 minimize the "hearing" and maximize 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. Subsequent awareness sessions should then be limited to an hour at a time.

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 organization and its 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 appears follows. They cover all of the topics mentioned above and can be utilized 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 program, including slogans, posters or Good Security Practice, ideas should be asked for both at the workshop and at any time in the future.

Conclusion

It is imperative that senior management realizes 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.

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.

Example slide content

The following is designed to be used in creating a security awareness program within your organization.

Introduction - Slide 1

Background

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

Employees are unaware of what constitutes an information asset or what their legal obligations are. Some users do not know the difference between a USERID and password. It is not commonly understood that the organization is the legal owner of its information and that the computer programs it develops are its intellectual property not the individuals.

In most organizations 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 organization
- Look at the broader definition of the concept of information and Information Security.
- Examine the threats facing organization and possible motives and other organizations tackling security in the rapidly changing world of information technology.
- Introduce the documentation being produced for protecting information.
- And look at the ways in which you can help in securing organization information assets, which will ensure organization 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 both for you, your colleges and the organization 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

Organizations 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 organization relies on the availability and accuracy of its information systems in order to support its key business functions and to maintain its level of service to its customers and dealers.

Information Processing Is No Longer Centralized

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

- Information processing is no longer centralized – even when there is a centralized server
- Information processing has moved from a centralized 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!
- The proliferation of personal computers has revolutionized the availability of computing power and many of companies are moving towards distributed processing where the mainframe is used mainly as a central database.
- This has however posed a considerable challenge of ensuring the integrity and availability of the information on which organization depends on to service its business units, as decentralization 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 are unaware of what constitutes an information asset or what are their legal obligations. Some users do not know the difference between a USERID and password. It is not commonly understood that the organization is the legal owner of its information and that the computer programs it develops are its intellectual property not the individuals.

Legal requirements

There are various legal requirements that are incumbent on businesses such as organization 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 organizations 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.

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 don't mention.

- Raw data
- Word-processing
- Output reports
- Electronic Mail
- Programs
- Communicated Records
- Faxes
- Recorded on Disks and USB Keys
- Spoken and written word

Information is now considerably more portable and more accessible. Imagine trying to carry a four drawer filing cabinet in your brief case or handbag, when it can all be contained on a USB key or 1 DVD. 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 programs specifications. Imagine how useful that would be to someone who wanted to disrupt the organization.

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 at a reasonable cost:

- modification,

- disclosure,
- destruction,
- denial,

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 and 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 organization 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, we now have visual access to considerably more information than we previously had.

Threats - slide 7

Information such as strategic, administrative and financial concerning organization, products, services and personnel, has always been a vital resource for organization. But 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 organization and directly for their own job security. It is also vulnerable to the business criminal and those who wish to do organization harm.

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

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

1. Human
2. Environmental
3. Natural

Human

- Internal
  - Errors and omissions
  - Disgruntled employees
- External
  - Competitors

- Current
- Potential
- Organized Crime
- Political Terrorists
- Hackers

Threats – slide 7 - 9

Internal Threats

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 organization are from human errors, accidents and omissions. The loses through errors accidents and omissions can comprise:

- changing the production version of a program 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;
- Failing to copyright a proprietary program;
- 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 being made redundant, drug or alcohol dependencies and gambling debts. The 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.

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 Threats

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

- Damage to the organization

Threats - slide 15

Environmental/Natural

- Information processing is no longer centralized
- Information processing has moved from a centralized 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!
- The proliferation of personal computers has revolutionized the availability of computing power and many of companies are moving towards distributed processing where the mainframe is used mainly as a central database.
- This has however posed a considerable challenge of ensuring the integrity and availability of the information on which organization depends on to service its business units, as decentralization 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 2000's

Threats - slide 16

Natural

The threats of natural disasters is a real one and recent examples should be included. Even in Australia we have had many such problems:

- Apple Computers affected by the April 2nd 1992 storms with flood damage;
- Large Insurance company roof collapse under weight of hailstones in 1990 in Sydney storm in the western suburbs;
- Australian Stock Exchange flooded in basement computer room;
- Lightning strikes affecting power supply for IBM and other computer users;
- Newcastle Earthquake;
- Manufacturers Mutual Basement flooded by corroding water pipes.

Motives - slide 17

Motives

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

Financial gain

Political

To attack another company

Personal Prestige

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

* Use where applicable.

Targets - slide 18 - 19

Why would organization be a target?

The organization is seen as a [e.g. - *government institution*],

It is involved with minority groups,

NOTE: consult with management and business groups to ensure other relevant reasons are included.

List those threats specific to your organization

NOTE: consult with management and business groups to ensure relevant threats are included.

Information security documentation - slide 20

The Information Security Policy applies to all organization information systems not just to those provided by ITS. 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 organization 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 organization Information assets not just those on the main frame.
- 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. For the purpose of the information security standards is defines the minimum standards, which should be applied for handling organization 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 organization Information Assets.

Information Security Procedures

Procedures can be defined as a particular course or mode of action. They describe an act or manner of proceedings in any action or process. The procedures explain the processes required in requesting USERIDs, password handling, and destruction of information. The procedures for requesting USERIDs or access changes will be conducted in the future via E-mail with easy to use templates that prompt the requester for all the information required. Requests can be expedited in a matter of minutes providing greater productivity for all concerned.

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 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 at the moment 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.

Frequently Asked Questions

While the policy document and the standards and procedures have in most cases tried to minimize 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 hopefully covering 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

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 organization to lose credibility and you could affect your job. Good security assists in the well being of the organization 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 work flow and can subsequently enhance productivity.

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

- information could be lost costing organization money to recreate it;
- management could make a bad decision based on incorrect information;
- giving out private information could cause the organization embarrassment. As a result organization may end up in litigation;

- a rival may obtain company information causing organization to lose competitive advantage.

People Are Important Too

The organization recognizes that the employees are its most important asset. The safety and security of the employees is paramount to the management. There are many ways in which organization seeks to ensure the security and safety of its employees by various security, health and safety programs. Security whether it is physical or logical is important both for you and the company and the policies and procedures exist to protect both organization and you. The role you have to play in the well being of organization should not be underestimated, as you are the key to its success.

There are many ways in which you can assist in Good Security Practices such as:

- protecting Information In Your Work Area (clear desk etc);
- password and USERID Controls;
- software Use;
- good Backup Procedures;
- using organization 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 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, Don’t use them or leave then on public transport and don’t let your children play with them.

Secure Disposal Of Information

Some of the methods which 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 disks have sensitive information on them, cut them in half before disposing of them; and
- if a disk 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, willful 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 organization.
- 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 organization.

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

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 ITS Security and control even though you may be tempted. This is for your own protection and to guard against any possible recriminations should the suspicion prove to be proven or unfounded. This point cannot be overemphasized.

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 IT.

Any suspected reported breach will be treated with the utmost confidence and will precede no further if proved to be 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 are handled with care:

- Network diagrams
- Internal telephone directory
- Organizational charts

There Are Legal Reasons Why You Should Protect organization 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;
- Prohibiting violations of copyrights, patents and trade secrets;
- Prohibiting unauthorized computer access;
- Protecting the privacy of an individual’s personal information (social security number, tax file number, etc.). Breaching the security and control procedures is a serious matter and more serious cases 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 authorized access to it all the time, but it is important to prevent access by unauthorized 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
- Challenge unauthorized visitors.

Do not read sensitive information on public transport.

- Ensure that anyone you see using a workstation in your area is authorized to do so.
- When sensitive information is on the screen, make sure that no one else can see it. This is especially important if it is an area where you receive members of the general public, make sure 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 your company;
- Sales people and organization clients.
- refer any questions from the media (reporters) to the appropriate people in organization;
- 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 organization telephone book. This would allow them to make calls which others in organization 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 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;
- 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 organization and cannot be copied by you if:

- you use company equipment to develop it;
- you develop it on behalf of organization;
- you develop it on organization time regardless of the equipment you used.

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

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

‘Borrowing’ Software

Taking copies of software depends on the software and the license agreement with the vendor permits it. 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.

- obtain your managers approval before copying software;
- although organization may have purchased the software it will probably be licensed for use on one machine only;
- Unauthorized copying of software is a criminal offence. It is critical for your own protection as well as organization 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 copying 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 the original diskette make a backup copy and use great care in protecting the diskette from damage.

Using the organization’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;
- make sure you have insurance coverage;
- Use extra care in handling the equipment, 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;
- make backup copies and protect them the same as the originals;
- protect the information from damage and protection;
- protect the information from observance by unauthorized 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 organization’s insurance policy does not cover the equipment if stolen;
- If it is stolen organization will not replace it.

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, D.C, 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.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program 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 its 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 that may have already impacted the way in which you conduct your work and most certainly may do 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 which were used as identification techniques in science fiction movies and for the military are now gaining acceptance in 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 authorizations 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 digitized signature and not a finger print.

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 these threats can take many forms, 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 its 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 organization to provide the efficient reliable and quality services both to its customers, business partners and employees would be severely hampered. The need arises for a coordinated approach in designing and implementing a security program that will provide flexible cost effective solutions while still protecting organization 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 its value both within the organization and outside of it; whether it is with friendly or hostile parties.

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

This will depend on your organization's requirements as they may not want certain types of document given out, or they may want copies of security policies, Intranet web site addresses etc given.

System Improvement Monitoring and Checks

In order to ensure this programs success, it is necessary to monitor the following key areas using appropriate metrics:

1. Approval for adequate funding has been obtained,
2. Senior management supports and evangelizes the program
3. Organizational metrics indicate a reduction in the number of incidences and security violations within the organization,
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 organization will include:

1. Random “spot checks” of behavior 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 organization has been accessing this material, and what level of comprehension they are retaining.

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

System Maintenance

The “Check” phase of this program needs to provide an effective evaluation and feedback in a manner, which will allow a process of continuous improvement. For the program to remain effective, the process of continual improvement must be implemented.

A variety of parties must be involved in the ongoing assessment of the awareness and training program:

- **Senior management** – need to provide support through strategic planning. The support of senior management is critical to the success of these programs. Through evangelizing the program, senior management helps ensure the program’s uptake and success.

- **Information security manager** – can help identify training sources, evaluate the effectiveness of awareness and training programs 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 organization’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.

Some approaches to solicit feedback detailing the programme include:

- Initiation of an external audit process, an independent external body may often provide additional insights to the process.

- Status reports from management, individual management has day to day today knowledge of the needs of the organization from a smaller scale viewpoint. A compilation of these manager reports to help improve the overall organization's security standards.

- Program benchmarking, benchmarking (either internal or external) is an effective method of rating the program 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 program 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:

1. Are the skills required by the personnel working on information security adequate / current,

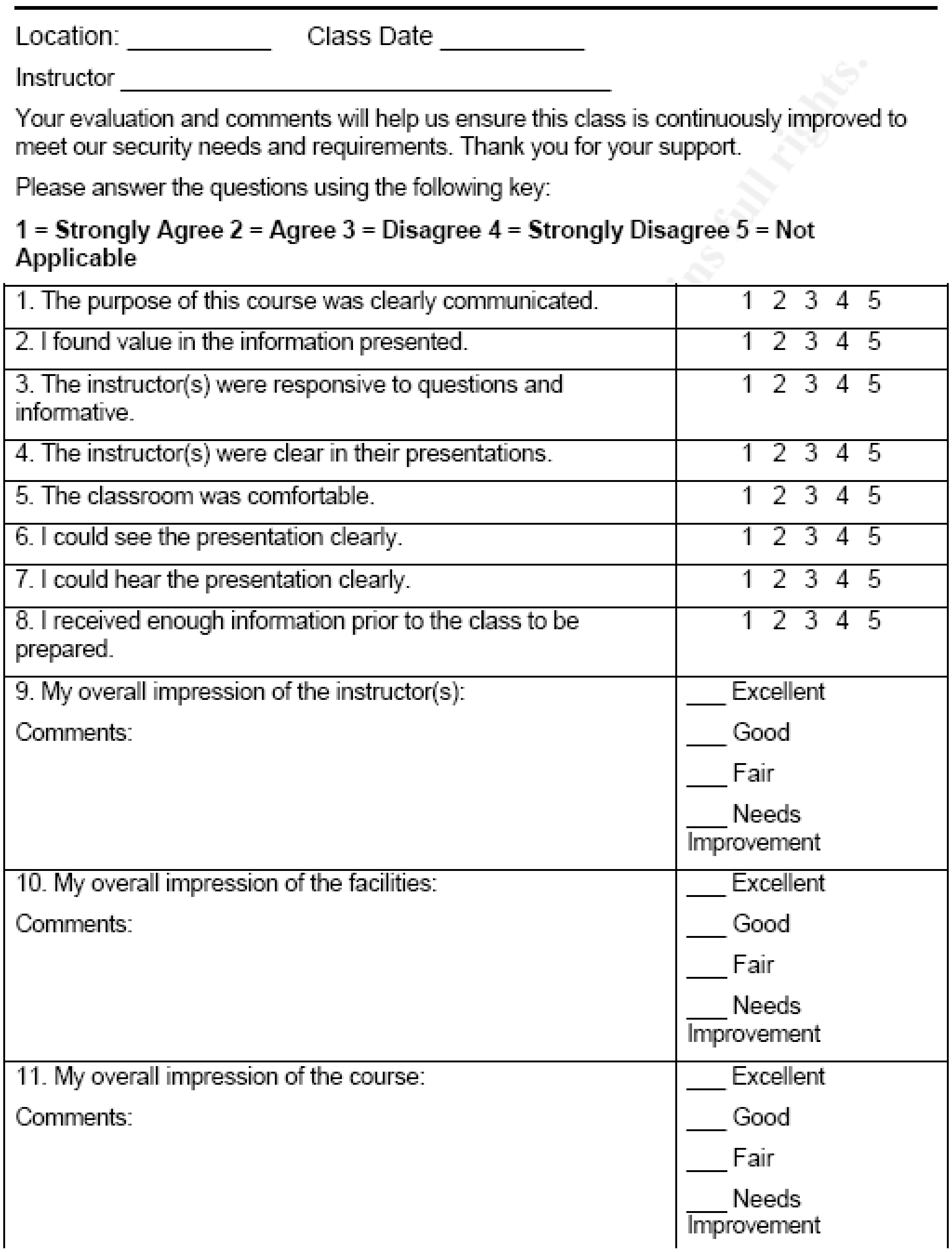
2. Is the training appropriate for the organizations needs and, is it necessary to hire experienced staff for specific tasks,

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 organization?

Testing Knowledge and Security Awareness

It is essential to monitor and review the awareness program for it to be successful. This process is a combination of reviews from the user, management, finance and HR. On top of the evaluations, periodic user quizzes are a great idea. These allow you to gain feedback on how much the organization has really learnt.



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

Figure 2, Example - Security Awareness Evaluation Form

Sample Managerial assessment interview questionnaire

The following are a few questions that may be asked in order to assess an awareness program.

1. 1 Is a current information security awareness program 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 fulfill them?

2. 2 Is the program approved by senior management?

3. 3 Does the process specify timeframes and re-training requirements?
4. 4 Is it fully documented?
5. 5 Are new employees trained within 30 days of being hired?
6. 6 Do all employees sign that they have understood and accept the training and organizational policies?
7. 7 How often is refresher training provided?
8. 8 Does your staff know what's expected of them in their role regarding security for the organization, and your division?
9. 9 When did you last attend a security workshop for staff provided by the Security Division?
10. 10 Is our contract is included in security awareness sessions?
11. 11 What areas do the awareness training cover (e.g. password practices, use of anti-malware)?

Conclusion

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

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

A security awareness program should be an ongoing program 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 following the 911 incident and the ensuing actions in the subsequent years emphasize 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.

Our people are our first line of defense – no matter what type of organization we work for. The successful implementation of an awareness program is critical to the success of the entire information security program as a whole. This chapter has detailed many of the procedural steps needed for the development of an awareness program focused on the provision of security awareness and training systems within the organization.

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 compliance.