Cyber Security
Unit - I

Dr. R. A. ROSELINE M.Sc., M.Phil., Ph.D.,
Associate Professor and Head,
Post Graduate Department Of Computer Applications,
Government Arts College, Coimbatore – 18.

CYBER SECURITY [18 MCA 5 1 C]
SYLLABUS

UNIT I:

Threats to Information Security: What is information Security? – Common threats. **The structure of an Information Security Program:** Overview – Business Unit Responsibilities – Information Security Awareness Program – Information Security Program Infrastructure.

(Book 1 | Chapter 2 & 3)

UNIT II:

Information Security Policies: Policy is the Cornerstone – Why Implement an Information Security Policy – Corporate Policies – Organization wide (Tier1) Policies – Organization wide Policy Document – Legal Requirements – Business Requirements – Definitions – Policy Key Elements – Policy Format.

(Book 1 | Chapter 4)

CYBER SECURITY [18 MCA 5 1 C]
SYLLABUS

UNIT III:

Asset Classification: Introduction – Overview – Why Classify Information? – What is Information Classification? – Where to Begin? – Information Classification Category Examples – Resist the Urge to Add Categories – Constitution of Confidential Information – Employee Responsibilities – Classification Examples – Declassification of Information – Records Management Policy – Information Handling Standards Matrix – Information Classification Methodology – Authorization for Access.

(Book 1 | Chapter 5)

UNIT IV:

Access Control: Business Requirements for Access Control – User Access Management – System and Network Access Control – Operating System Access Control – Monitoring Access Control – Cryptography. **Physical Security:** Data Centre Requirement – Physical Access Control – Fire Prevention and Detection – Verified Disposal of Documents – Agreements – Intrusion Detection Systems.

(Book 1 | Chapter 6 & 7)

UNIT V:

Information Security and Cyber Law: Introduction – Objectives – Intellectual Property Rights – Strategies for Cyber Security – Policies to Mitigate Cyber Risk – Network Security – IT Act – Signatures – Offence and Penalties.

(Book 2)

TEXT BOOKS:

1. Thomas R. Peltier Justin Peltier, John Blackley, "*Information Security and Fundamentals*", Auer bach Publications.
2. "*Information Security and Cyber Law*", Tutorials Point Simply Easy Learning, **www.tutorialspoint.com/information_security_cyber_law/information_security_cyber_law_tutorial.pdf** (E-book).

REFERENCE BOOKS:

1. Bhushan, Rathore, Jamshed, "*Fundamentals of Cyber Security*", First Edition, BPB Publication, 2017.

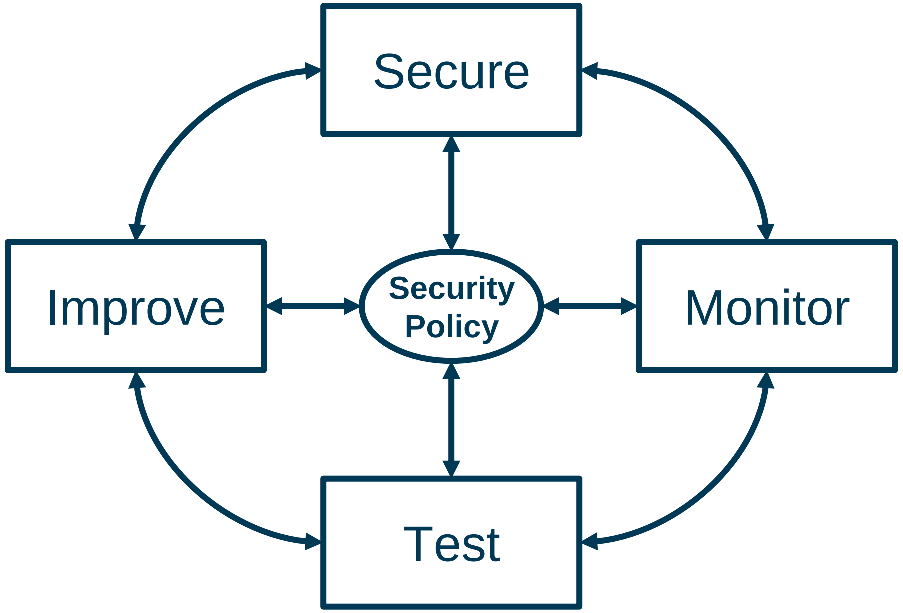
Contents

1. **Threats to Information Security**
    a. What is information Security?
    b. Common threats
2. **The structure of an Information Security Program**
    a. Overview
    b. Business Unit Responsibilities
    c. Information Security Awareness Program
    d. Information Security Program Infrastructure

Information Security

1. Information Security refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption.
2. The purpose of information security is to protect an organization's valuable resources, such as information, hardware, and software.

- The first and probably most important aspect of information security is the security policy.
- If information security were a person, the security policy would be the central nervous system.
- Policies become the core of information security that provides a structure and purpose for all other aspects of information security.



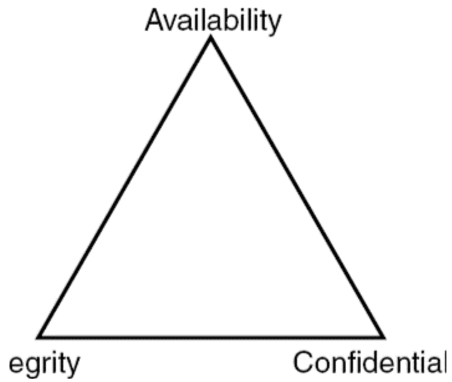
1. Access control can be implemented in many different parts of information systems. Some common places for access control include:
    1. Routers
    2. Firewalls
    3. Desktop operating system
    4. File server
    5. Applications
2. Some organizations create something often referred to as a “candyland.”A “candyland” is where the organization has moved the access to just one or two key points, usually on the perimeter. This is called a “candyland” because the organization has a tough crunchy exterior, followed by a soft gooey center.

1. Patch management would be a task from the maintenance part of system development and maintenance.
2. This is a task that has many information security professionals referring to themselves as “patch managers.”
3. With such a large number of software updates coming out so frequently for every device on the network, it can be difficult — if not impossible — for support staff to keep everything up-to-date.

Common Threats

1. From the hacker sitting up until all hours of the night finding ways to steal the company's secrets, to the dedicated employee who accidentally hits the delete key, there are many foes to information security.
2. Due to the many different types of threats, it is a very difficult to try to establish and maintain information security.

- The information security triad shows the three primary goals of information security: integrity, confidentiality, and availability. When these three tenets are put together, our information will be well protected.



CIA Traid

1. Errors and Omissions

1. While error and omissions do not get the headlines of international hackers and the latest work propagating through the e-mail system, it is still the number-one threat to our systems.
2. Errors and omissions attack the integrity component of the CIA triad. To help fight these mistakes, we can use some of the following security concepts.

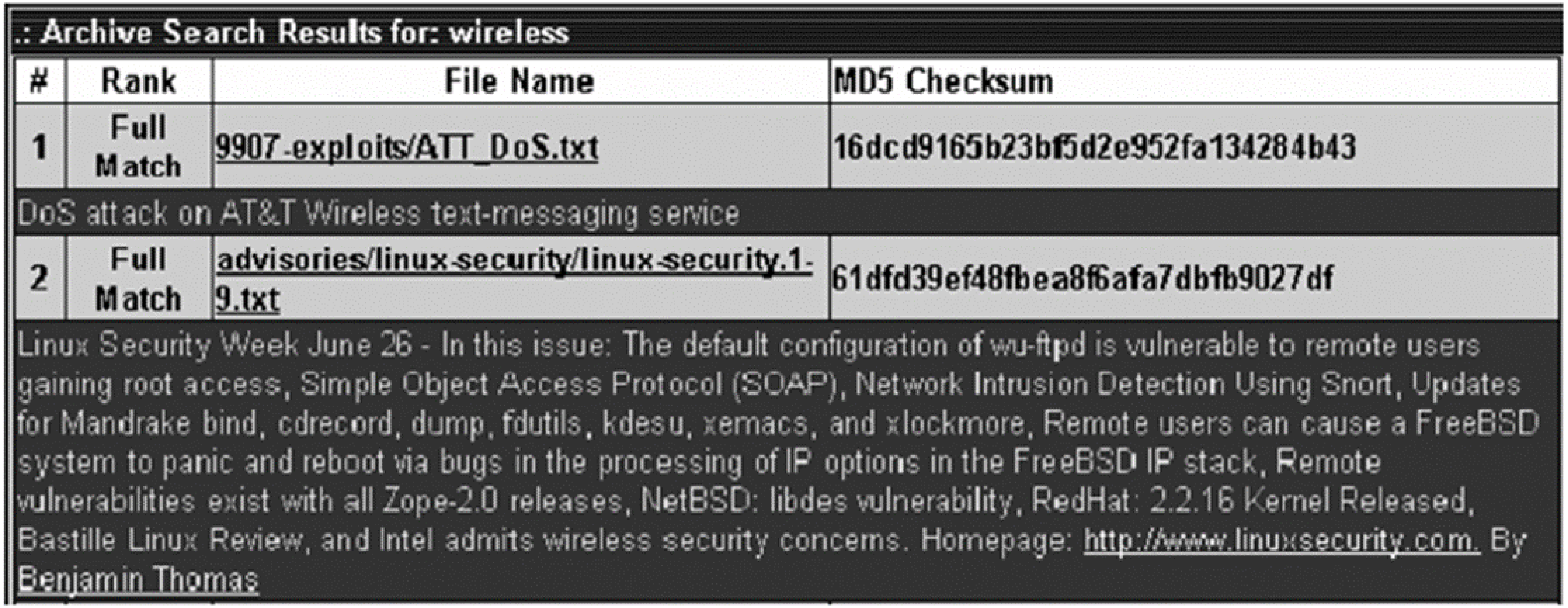
2. Fraud and Theft

1. If your end users are not accidentally destroying data but are maliciously destroying the information, then you may have a completely different type of attack.
2. All data recovery processes performed on the system will also be performed on the backup copy of the hard drive.
3. Once the copy is made, a comparison of the hard drives will be done using an integrity technology called an MD5 hash

MD5

The definition of an MD5 hash, as taken from the MD5 Web page, is as follows:

1. [The MD5 algorithm] takes as input a message of arbitrary length and produces as output a 128-bit “fingerprint” or “message digest” of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest.
2. In essence, MD5 is a way to verify data integrity, and is much more reliable than checksum and many other commonly used methods.



.: Archive Search Results for: wireless

#	Rank	File Name	MD5 Checksum
1	Full Match	9907.exploits/ATT_DoS.txt	16dcd9165b23bf5d2e952fa134284b43
DoS attack on AT&T Wireless text-messaging service			
2	Full Match	advisories/linux-security/linux-security.1-9.txt	61dfd39ef48fbea8f6afa7dbfb9027df
Linux Security Week June 26 - In this issue: The default configuration of wu-ftpd is vulnerable to remote users gaining root access, Simple Object Access Protocol (SOAP), Network Intrusion Detection Using Snort, Updates for Mandrake bind, cdrecord, dump, fdutils, kdesu, xemacs, and xlockmore, Remote users can cause a FreeBSD system to panic and reboot via bugs in the processing of IP options in the FreeBSD IP stack, Remote vulnerabilities exist with all Zope-2.0 releases, NetBSD: libdes vulnerability, RedHat: 2.2.16 Kernel Released, Bastille Linux Review, and Intel admits wireless security concerns. Homepage: http://www.linuxsecurity.com. By Benjamin Thomas			

FIGURE 2.3 Web Site with MD5 Values

3.Malicious Hackers

1. There are several groups of Internet users out there that will attack information systems.
2. The three primary groups are hackers, crackers, and phreaks.
3. While common nomenclature is to call all three of the groups “hackers,” there are some differences between the groups.

1. A hacker is a user who penetrates a system just to look around and see what is possible.
2. The etiquette of hackers is that after they have penetrated the system, they will notify the system administrator to let the administrator know that the system has a vulnerability.
3. It is often said that a hacker just wants security to be improved on all Internet systems.
4. The basic hacker methodology has five main components: reconnaissance, scanning, gaining access, maintaining access, and covering tracks.

1. A cracker has no etiquette on breaking into a system. Crackers will damage or destroy data if they are able to penetrate a system.
2. The goal of crackers is to cause as much damage as possible to all systems on the Internet.
3. The last group, phreaks, tries to break into an organization’s phone system.
4. The phreaks can then use the free phone access to disguise the phone number from which they are calling, and also stick your organization with the bill for long-distance phone charges.

4.Malicious Code

1. While malicious users can attack your system, programs released by the same group of people will often be more successful in reaching the protected parts of your organization.
2. Malicious code is defined as any code that is designed to make a system perform any operation with the knowledge of the system owner.

1. There are many different types of malicious code. This chapter discusses a few of the more common ones, including virus, worm, Trojan horse, and logic bomb.
2. The most commonly thought of type of malicious code is the virus.
3. A virus is a code fragment, or a piece of code, that can be injected into target files.
4. A virus then waits, usually until the file is opened or accessed, to spread to another file where the malicious code is then injected into that file.

1. With a virus-infected system, one can often find in excess of 30,000 infected files.
2. There are many different types of viruses; there are viruses that attack the boot sector of the hard drive, there are file system infectors, there are macro viruses that use the Office scripting functionality, and there are viruses for all major operating systems.

5. Denial-of-Service Attacks

1. The denial-of-service or DoS attack is designed to either overwhelm the target server's hardware resources or overwhelm the target network's telecommunication lines.
2. For years there were a number of common "one-to-one" DoS attacks. In these attacks, the hacker would launch an attack from his system against the target server or network.
3. Syn floods, Fin floods, Smurfs, and Fraggles are all examples of these "one-to-one" attacks.

6.Social Engineering

1. Social engineering is the name given to a category of security attacks in which someone manipulates others into revealing information that can be used to steal data, access to systems, access to cellular phones, money, or even your own identity.
2. Gaining access to information over the phone or through Web sites that you visit has added a new dimension to the role of the social engineer.

1. The social engineering exploiter preys on qualities of human nature, such as:

    a. The desire to be helpful. We have trained our employees well. Make sure the customer is satisfied. The best way to a good appraisal is to have good responses from those needing assistance. Most of our employees want to be helpful and this can lead to giving away too much information.

    b. A tendency to trust people. Human nature is to actually trust others until they prove that they are not trustworthy. If someone tells us that he is a certain person, we usually accept that statement. We must train our employees to seek independent proof.

1. The fear of getting into trouble. Too many of us have seen negative reaction by superiors because verification of identity took too long or because some official was offended. Management must support all employees who are doing their assignment and protecting the information resources of the enterprise.
2. The willingness to cut corners. Sometimes we get lazy. We post passwords on the screen or leave important material lying out for anyone to see.

Common Types of Social Engineering

1. While the greatest area for success is human-based interaction by the social engineer, there are also some computer-based methods that attempt to retrieve the desired information using software programs to either gather information or deny service to a system.
2. Other forms of social engineering have been classified into various groups. The first two are Impersonation and Important User.

1. Some potential security breaches are so mundane that they hardly seem to be a concern. With all the fires that we have to fight each day and the deadlines we have to meet, sometimes the most obvious are often overlooked:
2. Passwords. The number-one access point for social engineers is the good old-fashioned password. After all of the awareness programs and reminder cards, we still find that employee-generated passwords are too short or too easy to guess. System-generated passwords are too long and employees have to write them down to remember them. Even today, some systems do not require that passwords be changed.

1. Modems. Every company has more modems than they know about. Employees and contractors will add a modem to a system and then install products such as pcAnywhere or Carbon Copy to improve their remote access time. We recommend that war dialers be used at least twice a year to check on modems.
2. Help desk. Put in place processes that can assist the help-desk employee in verifying who is on the other end of the phone call.
3. Web sites. There are two problems here: the dummy site that gathers information and the legal site that gives away too much information.
4. Many hackers use the information they gather from the enterprise Web site to launch attacks on the network. Make certain that the information available will not compromise the information resources of the enterprise.

1. Because there is neither hardware nor software available to protect an enterprise against social engineering, it is essential that good practices be implemented. Some of those practices might include:
2. Require anyone there to perform service to show proper identification.
3. Establish a standard that passwords are never to be spoken over the phone.
4. Implement a standard that forbids passwords from being left lying about.
5. Implement caller ID technology for the help desk and other support functions.
6. Invest in shredders and have one on every floor.

1. Policies, procedures, and standards are an important part of an overall antisocial engineering campaign. To be effective, a policy should:
2. Not contain standards or directives that may not be attainable
3. Stress what can be done and stay away from what is not allowed as much as possible
4. Be brief and concise
5. Be reviewed on a regular basis and kept current
6. Be easily attainable by the employees and available via the company intranet

The Structure of an Information Security Program

1. The structure of an information security program is its performance at every level of the organization.
2. The reach of the program, how each business unit supports the program, and how every individual carries out his or her duties as specified in the program all determine how effective the program will be.

1.Enterprise wide Security Program

1. The aim of the information security practitioner should be to have a uniform information security program that spans the whole enterprise.
2. Many organizations have strong and weak areas; a good example might be a financial services organization in which everyone but the stock traders abides by strong information security standards.

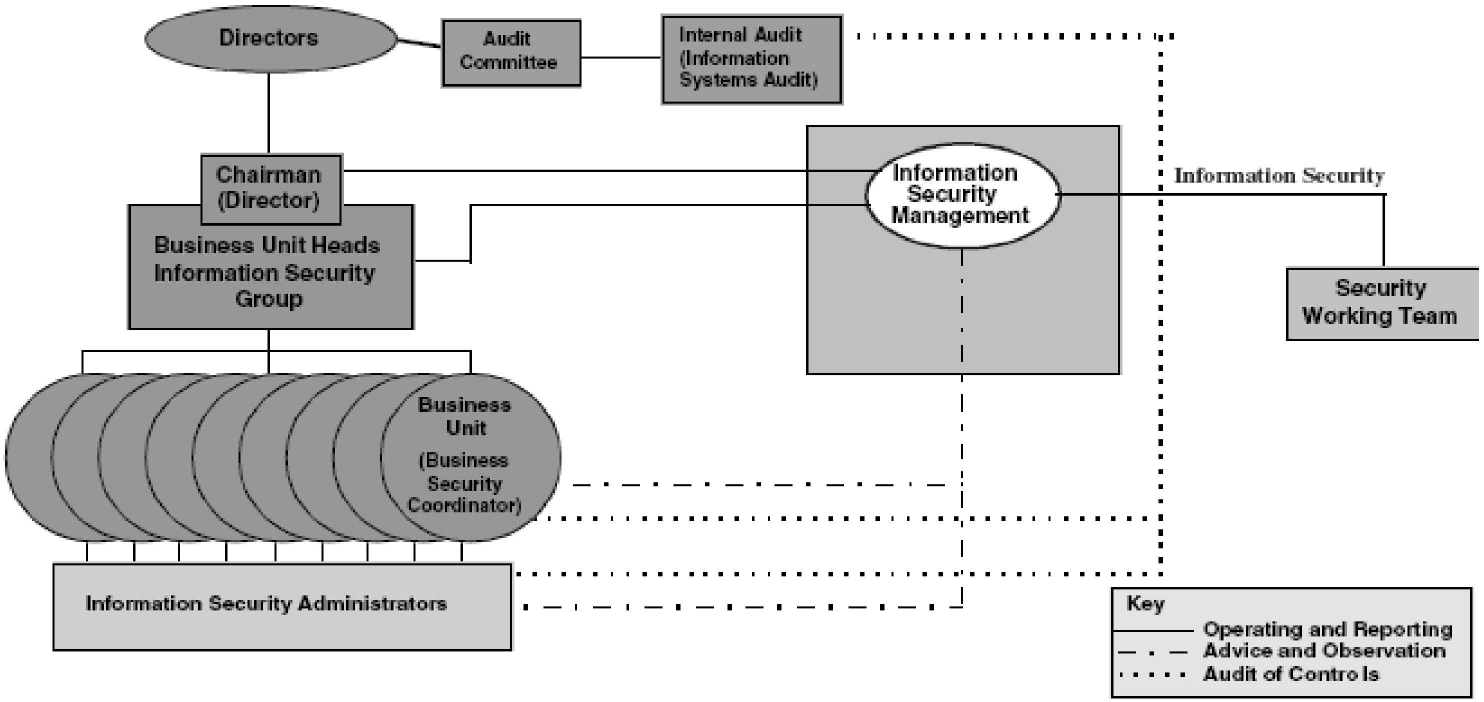

Directors
Audit Committee
Internal Audit (Information Systems Audit)
Chairman (Director)
Business Unit Heads Information Security Group
Information Security Management
Information Security
Security Working Team
Business Unit (Business Security Coordinator)
Information Security Administrators
Key
Operating and Reporting
Advice and Observation
Audit of Contro ls

FIGURE 3.1 Organization Structure

1. The organization structure should involve:
2. Information Security Management who provide direction for the program, advice to the entire organization, and a focal point for resolving security issues
3. Internal Audit who report on information security practices to the Audit Committee and, through the Audit Committee, to the organization’s directors and other senior management
4. A Steering Committee composed of the heads of all business units who — among their other duties — take direction from the organization’s senior management and make sure it is translated into working practices

1. Security Coordinators in each business unit who, with the support and cooperation of Information Security Management, implement the instructions of the steering committee
2. Security Administrators in each business unit who maintain the access controls and other tools used as controls to protect information
3. A Security Working Team that gets its support and direction from Information Security Management and the Steering Committee and that focuses on plans to implement new and amended information security processes and tools so that the implementation has the lowest possible impact on the organization

1. Of course, no information security practitioner should attempt to impose this structure on an organization where it clearly does not fit, but the broad responsibilities outlined above must be carried out if the information security program is to have robust support in the organization

Business Unit Responsibilities

1. Business unit responsibilities, it makes sense to separate them into two areas: the creation and implementation of policies and standards and compliance with those policies and standards.

Creation and Implementation of Policies and Standards

1. The development of policies and standards requires the involvement of every business unit.
2. Each business unit — at some point in its chain of authority to senior management — must be represented in the process to review and approve policies.

1. For the policies to be as robust as possible and to represent the needs of the entire enterprise, each business unit must be represented in two ways:
2. Some member of the chain of authority for each business unit must have the opportunity to approve policies (or withhold approval); and
3. A number of members of the chain of authority must be given the opportunity to review and comment on the policies.

Compliance with Policies and Standards

1. Moving beyond the drafting and implementation of policies and standards, each business unit — through its management — has the responsibility to ensure constant compliance with those policies and standards.
2. It is of little use to ignore information security policies and standards until an audit is performed and then have to devote a significant effort to remedial or “catch-up” work.

Information Security Awareness Program

1. The purpose of a security awareness program is in clearly demonstrating the "who, what, and why" of the policies and standards.
2. Reading alone is not the most effective method of absorbing information and, once read, the message of the policies and standards are easily forgotten in the stress of the working day.
3. If an organization wishes its policies and standards to have perpetual effect, it should commit to a perpetual program of reinforcement and information — a security awareness program.

1. Frequency

1. One of the main factors in the success of the employee information security awareness program will be the frequency with which the message is delivered to staff.

1. In the first year, you should aim to deliver the messages outlined above, plus messages on:
2. Information security standards
3. Information security monitoring
4. Information security performance measurement
5. More information security good practices
6. Of course, while delivering these messages, the employee information security awareness should also reinforce the original messages

2. Media

1. One of the main factors in the success of the employee information security awareness program will be the composition of the media used.
2. Each media element has its strengths and weaknesses and so media for delivery must be carefully selected to ensure that the message of the program is communicated as effectively as possible.
3. To rely on one medium — that is, video, posters, PowerPoint presentations, etc.

Information Security Program Infrastructure

1. The “infrastructure” discussed here is the mechanism within the organization that supports good information security practices. From the senior management who sit on the Information Security Steering Committee, to the responsibilities of every employee to practice good information security habits, the infrastructure must be robust and educated in order for the information security program to bring full benefit to the organization.

Information Security Steering Committee

1. the Information Security Steering Committee should ideally be comprised of senior managers (director or VP level) representing every major business element of the organization.
2. To round out the committee — to provide the best possible contribution at that level to the information security program — Internal Audit, Legal, Human Resources, and, where appropriate, organized labor should also sit on the committee.

Assignment of Information Security Responsibilities

1. Information security is an organization wide responsibility that touches every person. While the Information Security unit must act as a source of guidance and advice, the program can only succeed when all parties in the organization recognize their responsibility to protect information and exercise that responsibility.
2. The protection of information is no more than a part of doing business — as much a part as making sure that more tangible assets as, say, money in a bank or products made by a manufacturing company are physically protected.

Senior Management

1. Senior management personnel of any organization are the ultimate decision makers and, as such, have the ultimate responsibility for deciding how the organization will handle risk.
2. It is widely accepted that senior management, under the Foreign Corrupt Practices Act, has a responsibility to make sure that information security (as an element of risk) is adequately addressed in the organization.

1. senior management is responsible for:
2. Making sure that audit recommendations pertaining to the protection of information are addressed in a timely and adequate manner
3. Participating in the activities of the Information Security Steering Committee (where such a body exists) to guide the activities of the information security effort
4. Overseeing the formation, management, and performance of the information security unit; this includes providing adequate resources (budget, manpower, etc.) to make sure that senior management requirements for information security can be carried out.

1. Participating in the effort to educate the organization’s staff about their responsibilities for protecting information
2. Reviewing and approving information security policies and strategies for the organization
3. Providing resolution for information security issues that are of such magnitude or urgency that they must be addressed on an organization wide basis

Information Security Management

1. Information Security provides services and advice, but the responsibility for protection of information within those units lies squarely on the management and staff of those units.
2. In cases where conflicts arise because of differing opinions on how to implement information security measures, Information Security Management can be seen as an arbiter — or referee — of what is acceptable (acting, of course, under the direction of the organization’s senior management).

1. The Information Security Management of an organization must be able to:
2. Drive the effort to create, publish, and implement information security policies and standards. While the responsibility for the creation of policies and standards does not belong to Information Security Management, they should be best equipped to act as an agent to make sure these things are created and to project-manage the effort to implement.

1. Coordinate the creation and testing of business continuity plans. There is still some argument over whether or not business continuity planning ought to be a function of information security, and I recognize that there may be some environments where it is not desirable that information security and business continuity planning not be managed by the same organization. However, given the closeness of the objectives of information security and continuity planning, I wholeheartedly endorse the idea that business continuity planning is a function that should fall under the control of Information Security Management.

1. Manage the information security effort within the information security unit. Just as all business unit managers have the responsibility of making sure that information stored and processed by their unit is protected to a level equal to its value, so Information Security Management must take care of security databases and paper files, and protect them from threats.
2. Administer information security software tools on behalf of the organization. “On behalf of the organization” is a very powerful phrase here because no information security unit should make decisions about access to information.

1. The information is owned by other pieces of the organization and so the responsibility for deciding access rules lies with other parts of the organization. Information Security Management is only responsible for making sure that those access rules are implemented.
2. Provide enough education and awareness programs to the organization. This begs the question, “What is enough?,” and the glib answer is, “Whatever senior management decides is enough.” A
3. more useful answer, however, is that enough education and awareness is the amount that provides the information necessary for everyone in the organization to know what his or her information security responsibilities are

Business Unit Managers

1. Business unit managers support the information security program by:
2. Participating in the process of reviewing policies. Business unit managers must feed comments to senior management on every information security policy proposed for the organization, because it is the business unit manager who will enforce the policy within the unit.

1. Creating input for information security standards. Standards are more business-unit specific than policies (network support writes network security standards, Human Resources writes personnel security standards, etc.) and, with help from Information Security, business unit managers must write standards that their unit can live with and that adequately protect the information used by the unit.
2. Measuring information security within the unit. While Information Security will provide the metrics and the mechanisms for measuring the effect of the information security program, the business unit managers themselves benefit from taking responsibility for the measurement. Less negative audit comments and fewer disruptive events are two clear benefits from this kind of proactive stance.

1. Enforcing compliance with policies and standards. Information Security can report violations of policy and standards, but only business unit managers can initiate remedial and disciplinary action in response. Without such remedial and disciplinary action, policies and standards are soon seen as “toothless” and are ignored very quickly afterward.

1. Supporting information security education and awareness. The information security education and awareness program can only succeed with the clear cooperation of business unit managers. From basic cooperation in providing resources and scheduling events to a directive to adopt the messages delivered by the program, business unit managers' support is crucial. Making sure resources are available to draft, test, and maintain business continuity plans under the coordination of the Information Security manager or the IS manager's designee.

First Line Supervisors

1. Monitor their employees’ activities in light of organization information security policies and standards — directing better compliance where appropriate and reporting incidents of noncompliance to business unit managers.
2. Communicate security issues to Information Security, senior management (through business unit managers), and through them to the Information Security Steering Committee.
3. In organizations where information security is included as a performance measurement, comment on individual employees’ performance with respect to information security at performance appraisal time.
4. Support the information security policy by reinforcing the messages contained in the education and awareness elements of the program.

Employees

1. When asked to describe the information security responsibilities of employees, it would be easy (but not helpful) to say, “Everything else” and in a sense it would be true. Generally, employees are asked to comply with information security policies and standards and little else.
2. information security programs only work well when all employees participate, and employees participate most willingly when they feel they have a real role to play.

Third Parties

1. Third parties (contractors, vendors, etc.) are responsible for complying with the information security policies and standards of the organization with which they are contracted or to which they provide goods or services.
2. Such contractual terms should be the subject of any service level agreement (SLA) between the purchasing organization and any contractor or vendor.

1. Where contractors or vendors operate in a site operated by the purchasing organization, they are subject to the same rules and methods of enforcement as full-time employees of the organization.
2. Where the contractors or vendors operate on their own or others’ premises, the contract should state that the purchasing organization has the right to audit the contractors’ or vendors’ information security programs at the times of the purchasing organization’s choosing.

Thank you

The contents in this E-Material are from,

Thomas R. Peltier, Justin Peltier, John Blackley,
“Information Security and Fundamentals”,
Auerbach Publications, 2004