Security Awareness and the Five Aspects of Security

Shift
Security simply used to protect information vs. Enabling business initiatives with security
Bolt-on/add-on structure to business process vs. Integrating security and controls into daily business processes
Security Solutions and Technology used to supplement core infrastructure vs.
Leveraging security technical solutions to enhance core infrastructure

Aspect SM (Security Management)
Keeping the business risks associated with information systems under control within an enterprise requires clear direction and commitment from the top, the allocation of adequate resources, and effective arrangements for promoting good information security practice across the enterprise.

High-level Control

Objective
Safeguarding information and systems, as well as other assets, requires security activity to be organized efficiently across the enterprise. Accordingly, this area covers the organizational arrangements for managing security across the enterprise and the security awareness, know-how and skills of individuals with authorized access to the organization's information, systems and other valuable assets.

Standard of Good Practice
Provide a top-down management structure and a practical mechanism for coordinating security activity across the enterprise.

High-level control should be exercised by top management via a high-level working group, committee or equivalent body.

Membership of the group should include top management, business managers, those in charge of computer / network facilities, legal, the person responsible for promoting good practice in across the enterprise and other stakeholders as dictated by the entities purpose and goals.
The group should meet at least three times a year to monitor the security condition of the enterprise, provide direction (such as by approving security standards and procedures) and coordinate security activity.

Driving Force

Objective
To actively promote good practice in information security and ensure that it is applied effectively across the enterprise.

Standard of Good Practice
A unit should be established, such as a specialist security function, which has an enterprise-wide responsibility for promoting good practice in security.
The specialist security function (or equivalent) should:
• Define a set of security mechanisms and supporting standards
• Be responsible for helping business managers, users, IT staff, and others to fulfill their security responsibilities, by providing expertise and running awareness programs
• Measure the effectiveness of security enterprise-wide

• Provide support for security classifications, risk analyses, audits, third party agreements and business continuity plans
• Monitor general business trends, technological developments, new threats /vulnerabilities (for example via the Internet) and new solutions (such as cryptography)
• Be run by staff who are equipped with the know-how, skills, resources and management support needed to fulfill their role.
The person in charge of the specialist security function (or equivalent) should have direct access to all levels of management throughout the enterprise and maintain contact with counterparts in the commercial world (including government or law enforcement agencies) and external security experts.

Local Coordination
Objective
To promote good security practice at a local level within the enterprise, and ensure that it is applied effectively.
Standard of Good Practice
The heads of business units / departments should be responsible for information security within their own areas.
Arrangements should be made to coordinate information security activity within each part of the enterprise.
Local security coordinators should be appointed in individual business units /departments. They should be equipped with the know-how, skills, time, tools, contacts and authority needed to fulfill their role. Local security coordinators should have access to in-house or external expertise in information security and be supported by standards /procedures for day-to-day security activities.
The condition of information security in all parts of the enterprise should be reported to the head of the enterprise-wide driving force for information security, in a consistent manner and on a regular basis.

Security Awareness

Objective
To ensure business and IT managers, users and others with access to the information and systems of the enterprise understand the key elements of security, why it is needed and their personal responsibilities.

Standard of Good Practice
Awareness of information security should be maintained via effective awareness programs covering all individuals with access to information or systems within the enterprise.
Employees (including contractors) should be provided with guidance to help them understand information security, the importance of complying with policies / standards and to be aware of their own personal responsibilities.
Formal awareness programs should be:
• Coordinated by a designated individual or group
• Run using structured education / training programs and specialized awareness material
• Supported by top management
• Kept up-to-date with current practices
• Applied to all individuals with access to information or systems.
The level of awareness within the enterprise should be measured and reviewed periodically.

Security Education
Objective
To equip personnel involved in controlling, using, running, developing and securing the information and systems of the enterprise with the knowledge and skills required to fulfill their security responsibilities.

Standard of Good Practice
Education / training should be provided to all personnel with control over, or access to, the organization's information, systems and other assets. This should equip all personnel with the know-how required to assess security requirements, propose security controls and ensure controls function effectively.
Education / training should also be provided to ensure that:
• Business users use systems correctly and apply security controls
• IT staff develop systems in a disciplined manner and run installations or communications networks correctly
• Information security specialists understand the business, know how to run security projects and can communicate effectively.

Electronic Mail

Objective
To ensure that: electronic mail services are available when required; the confidentiality and integrity of messages is protected in transit; and the risk of misuse is minimized.
Mail servers should be configured to protect the availability of electronic mail (e-mail) systems, by limiting the size of messages / user mailboxes, restricting the use of large distribution lists and preventing e-mail 'loops'.
Standard of Good Practice
E-mail messages should be scanned for:
• Known malicious code, including attachments where such code could be hidden
• Prohibited words, such as those that are offensive
• Key known phrases, such as those commonly used in hoax viruses or chain letters.
E-mail systems should be protected by:
• Blocking messages that originate from undesirable web sites or e-mail list servers, for example to help prevent 'spamming'
• Hashing messages to help maintain integrity and encrypting those that are confidential
• Ensuring non-repudiation of messages, for example to prove the origin of a message by
Using mechanisms such as digital signatures.
Users of e-mail systems should be warned that the contents of e-mail messages might be legally binding, messages sent or received may be monitored and misuse of e-mail facilities can result in disciplinary action.

Remote Working

Objective

To ensure that computers used by staff working in remote locations operate as intended, remain available and do not compromise the security of any facilities to which they can be connected.
Computers used by staff working in remote locations (typically desktop or laptop PCs) should be purchased from a list of approved suppliers, tested prior to use, supported by effective maintenance arrangements and protected by physical controls.

Standard of Good Practice
Computers used in remote locations should be:
• Equipped with standard configurations of system and application software
• Protected by the use of a comprehensive set of system management tools, access control mechanisms and up-to-date virus protection software
• Automatically logged-off after a set period of inactivity.
Staff working in remote locations, including from public areas, such as trains or airports or from home, should be:
• Authorized to work in specified locations

• Equipped with the necessary skills to perform required security tasks
• Made aware of the additional risks associated with remote working, including the increased likelihood of theft of equipment or disclosure of confidential information
• Provided with technical support
• In compliance with legal and regulatory requirements (for example, health and safety laws)
• Provided with alternative working arrangements in cases of emergency.

Additional controls should be implemented on workstations with the capability of connecting to the Internet, including the:
• Use of standard web browsers, with key software updates applied, and configured to prevent users from disabling security options
• Warning users about the dangers of downloading mobile code and the implications of accepting or rejecting 'cookies'
• Imposing strict disciplines on the downloading of mobile code.

Third Party Access

Objective

To ensure that access to the enterprise's information and systems by third parties (i.e. external organizations, such as customers or suppliers and members of the public) is only provided following rigorous review and formal approval.

Standard of Good Practice

Third parties (i.e. external organizations, such as customers or suppliers and members of the public) should only be granted access to information or systems within the enterprise following rigorous review.

All connections from third parties should be uniquely identified, approved by the business 'owner', recorded and agreed by both parties in a formal contract. A risk assessment should be carried out, agreed controls implemented and rigorous testing performed.

Standards / procedures for third party access should specify methods of:
• Ensuring that controls over third parties are commensurate with business risks
• Making third parties accountable for their actions
• Limiting liabilities and protecting ownership rights
• Complying with legal or regulatory obligations.

Standards / procedures for third party access should cover arrangements for:
• Achieving technical compatibility, logging activity and providing a single point of contact for dealing with problems
• Restricting methods of connection and the type of access granted
• Subjecting third party users to strong authentication
• Terminating connections when no longer required.

Individuals responsible for managing third party connections should have access to information about the risks associated with third party access, guidelines on how to secure connections, supporting tools such as checklists and sources of expertise for technical / specialist advice.

Aspect CB Critical Business Applications

A critical business application requires a more stringent set of security controls than other applications. By understanding the business impact of a loss of confidentiality, integrity or availability, it is possible to establish the level of criticality of an application. This provides a sound basis for identifying business risks and determining the level of protection required to keep risks within acceptable limits.

User Awareness

Objective

To maintain a high-level of awareness of information security among users of the application. Users of the application should be aware of a high-level information security policy, and comply with it.

Standard of Good Practice
Users of the application should be made aware of:
• The meaning of security and why it is needed
• the importance of complying with information security policies and applying associated standards / procedures
• their personal responsibilities for security
• particular security threats to the application.
Users of the application should be made aware that they are prohibited from:
• using any part of the application (such as modems) without authorization or for purposes that are not work-related
• making obscene, racist or otherwise defamatory statements, such as through the application, via e-mail or over the Internet
• illicit copying of information or software
• disclosing confidential information (such as network designs or IP addresses) or compromising passwords (such as writing them down or disclosing them to others).
Users should be advised that they should lock away sensitive media and documentation when not in use and log off the application if leaving a terminal unattended. They should be warned of the dangers of being overheard when discussing business information over the telephone, and in public places such as train carriages, airport lounges or bars.

Aspect IP Information Processing
Computer installations typically support critical business applications and safeguarding them is, therefore, a key priority. Since the same information security principles apply to any information processing activity - irrespective of where, or on what scale or types of computer it takes place - a common standard of good practice for information security should be applied.

Security Awareness

Objective
To maintain awareness of information security among individuals who run or use the computer installation.

Standard of Good Practice
Individuals involved in information processing activity should be aware of the high-level information security policy that applies across the enterprise, and comply with it. These individuals should include business ‘owners’, users and personnel who run the installation.
Individuals involved in information processing activity should be made aware of:
• The meaning of information security and why it is needed
• The importance of complying with information security policies and applying associated standards / procedures
• Their personal responsibilities for information security
• Particular security threats to the installation.
Individuals involved in information processing activity should be made aware that they are prohibited from:
• Using any part of the installation without authorization or for purposes that are not work-related
• Making obscene, racist or otherwise defamatory statements, for example through the installation via e-mail or over the Internet

• Illicit copying of information or software
• Disclosing confidential information (such as customer records, product designs or pricing policies).

Aspect CN Communications Networks
Communications networks convey information and provide a channel of access to information systems. By their nature, they are highly vulnerable to disruption and abuse. Safeguarding usiness communications requires robust network design, well-defined network services, and sound disciplines to be observed in running networks and managing security. These factors apply equally to local and wide area networks, and to data or voice communications.

Security Awareness

Objectives
To maintain awareness of information security among personnel who run the network.

Standard of Good Practice
Network staff should be aware of the high-level information security policy that applies across the enterprise, and comply with it.
Network staff should be made aware of:
• The meaning of information security and why it is needed
• The importance of complying with information security policies and applying associated standards / procedures
• Their personal responsibilities for information security
• Particular security threats to the network.
Network staff should be made aware that they are prohibited from:
• Using any part of the network without authorization or for purposes that are not work related
• Making obscene, racist or otherwise defamatory statements (using e-mail or other network services)
• Illicit copying of information or software
• Disclosing confidential information (such as network designs or IP addresses) or compromising passwords (such as writing them down or disclosing them to others).

Aspect SD Systems Development

Building security into systems during their development is more cost-effective and secure than grafting it on afterwards. It requires a coherent approach to systems development as a whole, and sound disciplines to be observed throughout the development cycle. Ensuring that information security is addressed at each stage of the cycle is of key importance.

User Procedures and Training
Objective
To ensure users are equipped to use systems correctly.

Standard of Good Practice

Users' responsibilities should be clearly defined. Users should be fully equipped to carry out their roles and supported by documented procedures, help facilities and training.
Users of new or significantly changed systems should be:
• Involved in - and contribute to - the development process
• Equipped with the know-how and skills to use systems correctly
• Formally trained.
User training should be carried out prior to systems going live and include information security tasks and responsibilities. User training programs should be signed-off by the project manager, the business 'owner' and a specialist in information security.