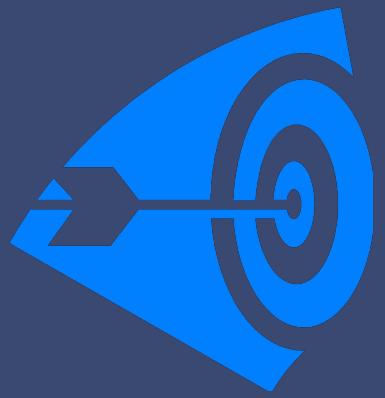
Course: Information Security Management in e-Governance

Day 2

Session 2: Security in end user environment

Agenda



- Introduction to IT Infrastructure elements in end user environment
- Information security challenges in end user environment
- Information security considerations and solutions for securing end user environment

Defining end users

End user environments are often characterized by a variety of people that

- Handle business information within and beyond the Organization's infrastructure
- Use technology that has been provided locally (eg finance software, USB memory sticks and mobile broadband cards)
- Configure their own desktop PCs and laptops (including the operating system)
- Make extensive use of the Internet for business and personal use
- Perform *ad hoc development and customization of business applications*

End users are typically employees who have access to and use technology to perform a particular role or function within the organization.

Defining end users - Characteristics

The level of technical skill, access to information and security awareness end users have also varies with individuals being:

- Regular everyday users
- Operational staff (with limited experience of technology)
- Technically competent users who configure software and build applications
- Mobile end users
- Individuals with special privileges (e.g. administrators and power users)
- Temporary staff (i.e. non-employees that perform a specific role for a short period of time).

Some of the Information assets at end user environment

- Desktop PCs, laptops, etc
- Portable storage devices
- Specialist equipment like scanners etc.
- Media

Factors affecting how end user environments are managed

The difference between an organization's corporate infrastructure and most end user environments can be significant, but often not apparent

A corporate infrastructure of enterprise-based applications, data centers and global networks is important in most organizations, often centrally controlled and well protected

However, the use and protection of business information can be heavily influenced by individuals in the end user environment, where much of the information resides, is processed and shared (often beyond the control of the corporate infrastructure)

Technology at end user environment

Technology represents an integral part of an organization's information processing capability.

End users make use of technology to:

Process information – using a wide variety of business applications such as:

- enterprise resource planning (eg SAP or Oracle)
- customer relationship management (CRM)
- commercial-off-the-shelf software (COTS)
- desktop applications

Technology at end user environment cont'd

Store information – using equipment such as:

- desktop PCs, thin-client devices, laptops, etc
- portable storage devices (eg external hard-disk drives, flash memory cards, USB memory sticks and media players with storage capacity)
- specialist equipment (eg scanning devices, bar code readers, data capture appliances and monitoring equipment)
- media (eg CDs, DVDs, magnetic tapes and computer disks).

Technology – contd..

Transmit information – using communication software that supports connectivity such as:

- local area networks (LANs) and wide area networks (WANs)
- wireless local area networks (WLANs) and Voice over IP (VoIP)
- Internet connections, Internet broadband and mobile (eg those used by mobile end users)
- direct connections to third party networks (eg using modem connections and leased lines)
- Bluetooth and infra-red.

Information security risks in end user environment

Risks associated with end user environment if not taken care of…..

Information in end user environments is subject to many different threats that can result in security incidents, with varying degrees of frequency and magnitude.

Common examples of threats include:

- Fraud (e.g. through modifying business information or creating false computer transactions / records)
- Theft of computer equipment, software and business information introduction of malware (e.g. viruses, spyware and worms)
- Downloading, storing or sending of inappropriate content (e.g. with obscene or discriminatory content)
- Information leakage (e.g. when replying to emails, sending documents and participating in teleconference calls)
- Deliberate disclosure of confidential information (e.g. by disgruntled employees or 'malicious insiders')

Risks associated with end user environment if not taken care of….. Cont'd

- Infrastructure failure (PCs, LAN, Printers, Scanners..)
- Human error (e.g. entering incorrect data into business applications)
- Social engineering attacks (e.g. by criminals that target employees to reveal confidential business information)
- Eavesdropping (e.g. when people are discussing a confidential topic)
- Shoulder-surfing (e.g. unauthorized individuals looking over the shoulder of people who are processing confidential information on the screen or reading confidential paperwork).

Challenges at end user environment

There are significant information security challenges that organizations currently face with many of their end user environments.

In particular, it is not unusual for management – at all levels within the organization (including senior executives) – to be unaware of the:

- Individuals or groups responsible for protecting information in the end user environment
- Types and importance of information handled in end user environments
- Wide range of threats to this information, which can – and often do – result in security incidents
- Real business impact caused when an incident occurs
- Extent to which critical and confidential information in end user environments is inadequately protected.

Impact of information security risks

Security Compromise : Outcome

- Theft and fraud
- Loss of confidentiality
- Loss of privacy
- Loss of integrity
- Loss of availability

Approach for securing end user computing infrastructure

Establish a security-positive culture in the end user environment

Ideal security measures

- Set objectives for security awareness in the end user environment
- Make end users aware of information risks
- Provide end users with actions for protecting critical and confidential information
- Monitor the behavior and security-related actions of end users

Threats and vulnerabilities addressed

- Human error
- Information leakage
- Loss of equipment containing confidential information
- Insider threat
- Tendency to share business information with Unauthorized parties
- Poor security behaviour

Establish a security-positive culture in the end user environment

- A security-positive culture is typically established by changing end user behavior, which often involves compulsory attendance at security awareness training etc.
- Make end users aware (e.g. as part of security awareness) that they are responsible for protecting business information they process, store and transmit.
- This includes when information is processed or stored on personal devices (approved or otherwise) or transmitted to external parties.
- Look for end user behavior that does not meet security requirements, often identified during security monitoring activities (e.g. non-compliance).

Establish a security-positive culture in the end user environment (cont'd)

Perform security monitoring of the end user environment, using a range of techniques (e.g. to help determine if policy is being complied with and awareness objectives are being adequately met).

- Participating in the review of the results of corporate monitoring activities that relate to the end user environment (eg reviewing end user access logs, unusual transaction activity, software failures and application availability)

- Carrying out regular audits / reviews to assess compliance with acceptable usage policies for business applications, equipment and connectivity

- Performing *ad hoc end user-based security assessments within the end user environment to determine the level of information protection* provided by end users

Information Protection Policy Measures…..

Understand who is the owner of critical and confidential information handled in the end user environment

- Classify and label confidential information (eg secret, restricted, internal or public) according to the organization's classification scheme or equivalent
- Maintain important details about confidential information (eg type and description, assigned level of confidentiality, physical / virtual location, name or role of the information owner and date for reclassification) in an information classification register

Information Protection Policy Measures…..

- Delete unwanted information (including electronic documents, emails and temporary web browser files) once they are no longer required or according to the document retention policy
- Comply with the organization's procedures for information security incidents (eg by reporting potential and actual to a specialized helpdesk)

Business applications Protection Policy Measures…..

- Use only approved corporate email and instant messaging services
- Download / install only approved software
- Read and comply with End User License Agreements (EULAs) for software installed by end users (where authorised)
- Use templates to create new electronic documents (not existing electronic documents that may contain confidential information)

Equipment Protection Policy Measures…..

- Maintain the security configuration and settings of equipment and software (eg by checking that virus protection software and personal firewall are in operation at all times and are prevented from being tampered with)
- Use file-based encryption, as a minimum, to protect individual confidential electronic files in storage and in transit (eg when saving to a portable storage device or sending via email or instant messaging)
- Protect information when storing on external hard-disk drives, flash memory cards and media (eg CDs and DVDs) by using encryption and storing the equipment in a secure location

Connectivity Protection Policy Measures…..

- Disable communication settings (eg wireless and Bluetooth) on mobile devices, such as laptops and smartphones, when not required
- Use secure web browser sessions (eg using SSL or TLS) where possible
- Encrypt confidential email before sending to recipients
- Use a virtual private network (VPN) when connecting to the corporate network from a remote location

Locations Protection Policy Measures…..

Adhere to the organization's ‘clear desk policy’ (or equivalent)

- Protect equipment and paper documents physically (eg by locking them away overnight and when not used during the day)
- Log off or lock desktop PCs and laptops (eg with a passphrase or PIN) to protect confidential information if leaving equipment unattended (eg during a meeting, lunch break or overnight)
- Challenge or report (eg to senior management or Physical Security function) unknown individuals in the end user environment who are not wearing an identification pass or acting in an unusual manner

Implement measures to protect critical and confidential information

Ideal security measures

- Determine the security measures required to protect each stage of the information lifecycle
- Apply manual controls for information handling

Threats and vulnerabilities addressed

- Information leakage
- Excessive privileges and access rights
- Disclosure or theft of confidential information
- Corruption of information
- Information located beyond the control of the Organization
- Excess of confidential information that has not been classified

Implement measures to protect critical and confidential information

Create

- Label information according to its level of classification (as indicated in the organization's information classification scheme)
- Record key properties (e.g. information owner and level of classification) within electronic documents (e.g. properties) and in an information classification inventory (or equivalent)

Implement measures to protect critical and confidential information..cont'd

Process

- Use validation routines in applications to help ensure critical information remains accurate (e.g. using data type checks, range checks, limit checks and presence checks)
- Process information in secure locations (e.g. offices with locked doors and access limited to specific individuals) to avoid unauthorized access to, or viewing of, confidential information
- Perform regular backups (e.g. by regularly saving electronic documents and configuring auto-save) to ensure critical information remains available at all times

Implement measures to protect critical and confidential information..cont'd

Transmit

- Use virtual private networks (VPNs) when connecting to the corporate network from a remote location
- Encrypt wireless networks used in the end user environment (whether they connect to a corporate network or not)
- Use secure web browser sessions (e.g. using SSL or TLS) where possible
- Encrypt confidential email before sending to recipients

Implement measures to protect critical and confidential information..cont'd

Store

- Use hard-disk encryption on desktop PCs and laptops
- Apply file-based encryption when storing confidential files on unprotected devices (eg USB memory sticks and external harddisk drives)
- Use encrypted USB memory sticks when transferring files between computers

Implement measures to protect critical and confidential information..cont'd

Destroy

- Destroy business information when it is no longer required (eg according to the organisation's document retention policy or equivalent)

- Use secure deletion software on computers, hand-held devices (eg smartphones) and portable storage devices (eg USB memory sticks and external hard-disk drives) to destroy information in electronic format

Implement measures to protect critical and confidential information..cont'd

- Degauss hard-disk drives and magnetic media where the stored information needs to be permanently destroyed
- Shred confidential paper-based documents and other correspondence or place in confidential waste bins
- Incinerate or physically destroy items such as hard-disk drives, portable storage devices and media (eg CDs and DVDs)

Deploy and protect approved end user equipment

Ideal security measures

- Acquire and use only approved equipment
- Apply software controls to endpoint devices
- Protect equipment against theft or loss
- Monitor the protective measures associated with equipment

Threats and vulnerabilities addressed

- Loss of availability of critical information
- Theft or loss of equipment
- Introduction of malware
- Poor practices around use of portable storage devices and hand-held devices
- Introduction of personally-owned equipment

Deploy and protect approved end user equipment

- Comply with corporate policy covering the acquisition and use of equipment to help ensure only suitable equipment is purchased and used within the end user environment.
- Provide standard builds for corporate-issued equipment (eg devices that use the identical hardware setup, the same type and version of operating system and software and are configured the same)
- Consult with the Information Security or IT function when acquiring equipment locally, particularly if it is not listed on the ‘approved list of equipment’ (or equivalent)
- Include protective measures (eg methods of backup, anti-virus software and personal firewall software) that end users can apply to their personally-owned equipment (including equipment at home).

Deploy and protect approved end user equipment (Contd)

Protect endpoint devices, such as desktop PCs, laptops and hand-held devices by applying a set of standard controls, such as:

- deploying hard-disk encryption or file-based encryption solutions to protect confidential information that is processed by, stored on or
- transmitted using the endpoint device
- restricting access (eg using password, token or biometric methods)
- filtering network traffic (eg personal firewalls)
- protecting against malware (eg deploying up-to-date anti-virus and anti-spyware software)
- backing up critical information at regular intervals (eg using automated backup software).

Develop and use desktop applications in a secure manner

Ideal security measures

- Maintain an inventory of critical desktop applications in the end
- user environment
- Implement a system development methodology for desktop
- Applications
- Review the development and use of desktop applications

Threats and vulnerabilities addressed

- Application failure
- Corruption of information in critical desktop
- Applications
- Lack of an inventory for critical desktop applications
- No system development methodology for critical desktop applications

Develop and use desktop applications in a secure manner (contd)

- Review desktop applications used in end user environment (with application owners, information owners or equivalent) to identify those that warrant a risk assessment
- Create an inventory of all critical desktop applications used in the end user environment.
- Record important details in the inventory of each critical desktop application
- Make the inventory of critical desktop applications available to the individual or group responsible for maintaining the corporate asset register for business applications
- Update details in the inventory as circumstances change, such as modifications to an application or a change in its level of criticality or classification

Develop and use desktop applications in a secure manner (contd)

- Segregate the roles associated with the development and use of critical desktop applications (to help reduce the likelihood of software bugs, human error and fraud)
- Comply with corporate policy for developing and using critical desktop applications (including the use of guidance and checklists).
- Store critical desktop applications in a central location to enable them to be protected in a consistent manner, for example by using access control, requiring passwords, performing encryption, creating audit trails and carrying out regular backups. E.g Network folder, database etc.
- Review and test critical desktop applications to verify that standards for their development and use have been followed

Develop and use desktop applications in a secure manner (contd)

- Perform independent audits of critical desktop applications prior to going live, and on a regular basis (using automated auditing tools where possible), for example by using a dedicated internal audit function or a specialist third party organization

- Review anomalies and issues regarding the development and use of critical desktop applications identified during security monitoring activities (eg non-compliance).

Restrict and monitor network connectivity

Ideal security measures

- Provide guidance on the use of network connectivity techniques
- Restrict the use of network connectivity in the end user Environment
- Protect network and telephony-based connectivity
- Monitor network traffic and connections

Threats and vulnerabilities addressed

- Unauthorized access to network equipment and
- networks
- Cracking of wireless encryption keys
- Eavesdropping of network communications
- Unavailability of network connectivity

Restrict and monitor network connectivity (contd..)

Comply with corporate policy (eg acceptable usage policies) for using network connectivity (including the use of guidance and checklists) in the end user environment.

This would typically cover:

- restricting connectivity (eg implementing access control on wireless access points, passphrase protection on telephony equipment and applying protective controls (eg encryption for transmitting information)
- monitoring the use of connectivity (eg using methods of intrusion detection, intrusion prevention and data loss / leakage protection).

Restrict and monitor network connectivity (contd..)

Restrict the number of network connection points accessible within the end user environment, for example by:

- keeping rooms with network access points locked
- connecting only the physical cables on network equipment (eg routers, switches and modems) that are required by equipment in the end
- user environment, and disconnecting them when no longer required
- concealing network cabling (eg to prevent tampering and unauthorised connection to the network).

Restrict and monitor network connectivity (contd..)

Restrict desktop applications from accessing the Internet (unless approved) to prevent vulnerabilities being exploited to provide unauthorized access to corporate computers and networks.

Examples of how to restrict applications accessing the Internet include:

- modifying functional properties within the application
- configuring a personal firewall (eg to block attempts by the application to connect over the Internet).
- Perform regular vulnerability assessments on networks associated with the end user environment to identify security weaknesses that malicious parties (eg hackers or disgruntled employees) may exploit.

Protect physical end user locations

Ideal security measures

- Protect end user locations
- Enable end users to apply physical protection techniques
- Perform regular reviews of the physical end user environment

Threats and vulnerabilities addressed

- Theft of equipment
- Eavesdropping private conversations
- Disclosure of confidential in papers
- Natural and man-made disasters

Protect physical end user locations (contd..)

Comply with corporate policy (eg an approved ‘clear desk policy’), standards and procedures for protecting physical locations covering the end user environment.

This is necessary to help provide physical protection of:

- end users who operate in each location
- equipment (eg desktop PCs, printers and videoconferencing kit) and media (eg CDs and DVDs) located in each location
- paper-based information (eg documents, reports and printouts) stored in each location.

Protect physical end user locations (contd)

Restrict access to confidential areas within the end user environment by a range of measures, including:

- physical access mechanisms (eg using card access, biometric systems or combination locks)
- restricted areas (by locked doors when unused)
- limiting access for visitors, and escorting them at all times.

Protect physical end user locations (contd)

Protect critical and confidential paper-based documents and media by:

- storing them in locked filing cabinets or fireproof safes
- adopting best practice for packaging and use of courier firms when sending them in the post (eg encrypting the information in the case of media and concealing the contents by using one envelope inside another)

Protect physical end user locations (contd)

Perform regular patrols of the end user environment to:

- check compliance with the organization's ‘clear desk policy’
- detect any unauthorized equipment (e.g. keystroke logging hardware, wireless access points)
- identify unattended computers that are logged on
- detect any unusual activity (e.g. tampering) associated with shared equipment, such as printers, facsimile machines and scanners.

Thank you