Glossary of Terms

Biometric Controls

Biometric controls are types of authentication devices used to confirm an individual’s identity. These controls are based on unique biological, behavioral and physical characteristics such as voice or fingerprint.

Cookie

A website (server) places one or more cookies on a hard disk to identify a user for future reference. A cookie requests that the user store the information (i.e., a website can remember information about a user). A cookie can monitor your actions on particular websites and record your preferences. The information stored by a cookie can be kept on the user’s computer. It is possible to view the cookie on your hard disk.
Digital Certificate
A digital certificate is a digital file issued to an individual or company by a certifying authority that contains the individual’s or company’s public encryption key and verifies the individual’s or company’s identity. (Turban et al., 2000, p. 507)

Digital Watermark
A pattern of bits inserted into a digital image, audio or video file that identifies the file’s copyright information (author, rights, etc.). The purpose of digital watermarks is to provide copyright protection for intellectual property that is in digital format. (webopedia.com)

Disk Operating System
Disk Operating System (DOS) refers to any operating system, but it is most often used as shorthand for MS-DOS (Microsoft Disk Operating Systems). Originally developed by Microsoft for IBM, MS-DOS was the standard operating system for IBM-compatible personal computers. (www.webopedia.com, 2003)

Electronic Commerce
Electronic commerce (e-commerce) is buying and/or selling products online. The payments are often in the form of electronic means. E-commerce can be business to business (B2B) or business to consumer (B2C).

Encryption
Encryption is a process of making messages indecipherable except by those who have an authorized decryption key. (Turban et al., 2000, p. 507)
Firewall
A firewall prevents unauthorized access to or from a private network, protecting the information and data in that network. Firewalls are installed in both the hardware and software to isolate a private network from intrusion from unauthorized public networks. All messages from an intranet pass through the firewall where any messages are reviewed. Those that fail to meet the security conditions for that network will be denied access.

Interoperability
Interoperability is the ability of a system to work with other systems to share information. The information shared allows both systems to operate more efficiently together.

Mobile Commerce
Mobile commerce (m-commerce) is any electronic transaction or information interaction conducted using a mobile device and mobile networks (wireless or switched public network) that leads to the transfer of real or perceived value in exchange for information, services or goods. (MobileInfo.com)

Public Key Infrastructure (PKI)
A public key infrastructure (PKI), also known as a trust hierarchy, allows Internet users to safely and securely exchange information and/or money via a trusted authority. PKI uses registration authorities such as digital certificates or certificate authorities to verify the individuals involved in an Internet transaction. Public key cryptography is the most common Internet method for verifying the message of a sender or encrypting a message. Two main types of cryptography are secret key and public/private key cryptography.
Secure Socket Layer

Secure Socket Layer (SSL) is an encryption method for transferring data between a client and a server. (Strategic Web Ventures.com)

Sniffer/Sniffing

A network manager uses a sniffer program to monitor network traffic. The obtained data is then analyzed for inefficiencies and/or problems on the network that can later be fixed by the network manager. A sniffer can also detect and read any information traveling along a network. A sniffer can be used to steal information from a network, putting a network at a security risk. For example, a sniffer program can find and share passwords.

Spam (or Spamming)

Spam is unsolicited mail, sent to a large number of e-mail addresses, often in the form of an ad or a scam. The sender views spam as a type of bulk mail obtained, for example, from a mailing list. Serious problems due to spam include: wasting bandwidth, wasting storage space and wasting time.

Spoofing

Spoofing is the creation of TCP/IP packets using somebody else’s IP address. Routers use the “destination IP” address in order to forward packets through the Internet, but ignore the “source IP” address. That address is only used by the destination machine when it responds back to the source. (Internet Security Systems)
References


