Office of the Minister
of State for Administrative Reform

Lebanese National Cyber Security Policy Guidelines

November 27, 2015

Document Details:

Publication Date	November 27, 2015
Review Date	November 24, 2015
Document Owner	Office of the Minister of State for Administrative Reform
Status	Final
Approved By	OMSAR
Approval Date	November 22, 2015
Version	1.7
Replaces	NA

Copyright© 2015

Disclaimer

The office of the Minister of State for Administrative Reform (OMSAR) hosts websites of many government entities such as the Presidency of Council of Ministers (PCM), the Internal Security Forces (ISF), the Ministry of Defense (MOD), the Ministry of Justice (MOJ), the Ministry of Energy and Water (MOEW), the Ministry of Public Health (MOPH), the Ministry of Agriculture (MOA), the Ministry of Environment (MOE) among others. In addition, OMSAR hosts different applications used by the public sector employees.

In 2012 the Presidency of the Council of Ministers (PCM) formed a National Cyber Security committee by issuing decision number 32 dated 25/7/2012 to develop a national and common strategy for the protection of the Lebanese governmental websites with shared responsibility among the different stakeholders. The committee was composed of members from the PCM, OMSAR, the Ministry of Interior and Municipality (MOIM), the Ministry of Economy and Trade (MOET), the Ministry of Defense (MOD), the Ministry of Telecom (MOT) in addition to the Central Bank of Lebanon (BDL).

After several meetings, the committee concluded in its final report No. 287/ص/2013 date 28/8/2013 with several recommendations. The second recommendation stipulated to:
"Commission the ICT Security Officer in OMSAR to work on and prepare a minimum set of security policy guidelines that should be adopted and implemented in all public agencies. These policy guidelines were required to conform to the international security standards."

Accordingly, OMSAR prepared a National Cyber Security Policy Guidelines document to be adopted and implemented in all Lebanese public agencies. The document is published on OMSAR's website and can be downloaded, referenced and adopted as a basis for creating secure data and information environment in the public administrations.

The document can be found at www.omsar.gov.lb/cybersecuritypolicy. These guidelines allow each public agency to create its own Cyber Security Policies based on the latest international standards and specifications.

The National Cyber Security Policy Guidelines document is complemented by a Security Checklist available from the same link. This Checklist enables the public agencies to assess their cyber security situation and lets them use it as a starting point to build their own security policies.

It is worth noting that this policy guidelines document is based on the Lebanese Standards NL ISO 27001 and NL ISO 27002 as adopted from the International Standards ISO 27001 and ISO 27002 by the Lebanese Standards Institution (LIBNOR).

Furthermore, the document applies the essentials of the Certified Information Systems Security Professional (CISSP) certificate by quoting from Wiley-Sybex's publications on this subject.

Preface

This document is intended to address the importance of having a written and enforceable Information Technology (IT) security policy, and to provide an overview of the necessary components of an effective policy. The reader will gain an understanding of the basic processes, methodologies, and procedures needed to initiate the development of an organization-wide IT Security Policy.

A security policy is a document that defines the security requirements for an organization. It identifies assets that need protection and the extent to which security solutions should go to protect them. Some organizations create a security policy as a single document and other organizations create multiple security policies with each one focused on a separate area (Stewart, Chapple, & Gibson, 2004).

When developing an IT Security Policy you should keep in mind the “defense in-depth” model. In other words, you should not be relying on one principal means of protection (or layer); instead, you should develop your security program so that it provides multiple layers of defense. This will ensure maximum protection of your data and resources and will minimize the potential for compromise.

Please keep in mind that we can only protect ourselves from known and existing exploits. We are all possible targets of zero day exploits! However, an effective IT security program will be enabling you to detect anomalies in network traffic and take the necessary steps toward mitigation. (Albright, 2002)

Contents

Security Policy Guidelines

1. Overview

Information Security provides protection to the information assets owned and managed by the government of Lebanon. It seeks to support the government's vision of delivering services that are effective, efficient and which add tangible value to Lebanon. The application of Information Security allows the government to promote an environment of trust that supports the transaction of the government's business. The achievement of effective Information Security requires active awareness and on-going participation on the part of government entities, citizens, residents and business partners.

The modern world is one in which there is an ever growing use of information assets and an ever increasing dependency on the information systems on which those assets reside. The Lebanese government has actively embraced that reality via a continuing program of e-Government initiatives. Such initiatives present a range of potential benefits but also bring with them new, complex risks that must be identified in a timely way and managed effectively (Abu Dhabi Systems and Information Centre, 2013).

2. Introduction

An IT Security Policy is the most critical element of an IT security program. A security policy identifies the rules and procedures that all persons accessing computer resources must adhere to in order to ensure the confidentiality, integrity, and availability of data and resources. Furthermore, it puts into writing an organization's security posture, describes and assigns functions and responsibilities, grants authority to security professionals, and identifies the incident response processes and procedures (Albright, 2002).

An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.

Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment. As a result of this

increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities.

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Whatever forms the information takes, or means by which it is shared or stored, it should always be appropriately protected.

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes.

Information and the supporting processes, systems, and networks are important business assets. Defining, achieving, maintaining, and improving information security may be essential to maintain competitive edge, cash flow, profitability, legal compliance, and commercial image.

Organizations and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Causes of damage such as malicious code, computer hacking and denial of service attacks have become more common, more ambitious, and increasingly sophisticated.

Information security is important to both public and private sector businesses, and to protect critical infrastructures. In both sectors, information security will function as an enabler and to avoid or reduce relevant risks. The interconnection of public and private networks and the sharing of information resources increase the difficulty of achieving access control. The trend to distributed computing has also weakened the effectiveness of central, specialist control.

Many information systems have not been designed to be secure. The security that can be achieved through technical means is limited, and should be supported by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail. Information security management requires, as a minimum, participation by all employees in the organization. It may also require participation from shareholders, suppliers, third parties,

> "If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."
>
> – *Bruce Schneier* – Chief Technology Officer of Resilient Systems

customers or other external parties. Specialist advice from outside organizations may also be needed. (NL ISO/IEC, 2010)

3. Security Management Planning

Security management planning ensures proper creation, implementation, and enforcement of a security policy. The most effective way to tackle security management planning is to use a top-down approach. Upper, or senior, management is responsible for initiating and defining policies for the organization. Security policies provide direction for all levels of the organization's hierarchy. It is the responsibility of middle management to flesh out the security policy into standards, baselines, guidelines, and procedures. The operational managers or security professionals must then implement the configurations prescribed in the security management documentation. Finally, the end users must comply with all the security policies of the organization.

Security management is a responsibility of upper management, not of the IT staff, and is considered a business operations issue rather than an IT administration issue. The team or department responsible for security within an organization should be autonomous. The information security team should be led by a designated Chief Security Officer (CSO) who must report directly to senior management. Placing the autonomy of the CSO and the CSO's team outside the typical hierarchical structure in an organization can improve security management across the entire organization. It also helps to avoid cross-department and internal political issues.

Elements of security management planning include defining security roles; prescribing how security will be managed, who will be responsible for security, and how security will be tested for effectiveness; developing security policies; performing risk analysis; and requiring security education for employees. These efforts are guided through the development of management plans.

The best security plan is useless without one key factor: approval by senior management. Without senior management's approval of and commitment to the security policy, the policy will not succeed. It is the responsibility of the policy development team to educate senior management sufficiently so it understands the risks, liabilities, and exposures that remain even after security measures prescribed in the policy are deployed. Developing and implementing a security policy is evidence of due care and due diligence on the part of senior management. If a company does not practice due care and due diligence, managers can be held liable for negligence and held accountable for both asset and financial losses.

A security management planning team should develop three types of plans:

> **Strategic plan**: A strategic plan is a long-term plan that is fairly stable. It defines the organization's security purpose. It also helps to understand security function and align it to goals, mission, and objectives of the organization. It's useful for about five years if it is

maintained and updated annually. Long-term goals and visions for the future are discussed in a strategic plan. A strategic plan should include a *risk assessment*.

Tactical plan: The tactical plan is a midterm plan developed to provide more details on accomplishing the goals set forth in the strategic plan. A tactical plan is typically useful for about a year and often prescribes and schedules the tasks necessary to accomplish organizational goals.

Operational plan: An operational plan is a short-term, highly detailed plan based on the strategic and tactical plans. It is valid or useful only for a short time. Operational plans must be updated often (such as monthly or quarterly) to retain compliance with tactical plans. Operational plans spell out how to accomplish the various goals of the organization. Operational plans include details on how the implementation processes are in compliance with the organization's security policy.

Security is a continuous process. Thus, the activity of security management planning may have a definitive initiation point. Effective security plans focus attention on specific and achievable objectives, anticipate change and potential problems, and serve as a basis for decision making for the entire organization. (Stewart et al., 2004)

4. Security Governance

Security governance is the collection of practices related to supporting, defining, and directing the security efforts of an organization. Security governance is closely related to and often intertwined with corporate and IT governance. The goals of these three governance agendas are often the same or interrelated – Transceiver.

Some aspects of governance are imposed on organizations due to legislative and regulatory compliance needs, while others are imposed by industry guidelines or license requirements. All forms of governance, including security governance, must be assessed and verified from time to time. Various requirements for auditing and validation may be present due to government regulations or industry best practices. The organization as a whole should be given the direction, guidance, and tools to provide sufficient oversight and management to address threats and risks with a focus on eliminating downtime and keeping potential loss or damage to a minimum.

Ultimately, security governance is the implementation of a security solution and a management method that are tightly interconnected. Security governance directly oversees and gets involved in all levels of security. Security is not and should not be treated as an IT issue only. Instead, security affects every aspect of an organization. It is no longer, just something the IT staff can handle on their own.

Security is a business operations issue. Security is an organizational process, not just something the IT geeks do behind the scenes. Using the term security governance is an attempt to emphasize this point by indicating that security needs to be managed and governed throughout the organization, not just in the IT department.

Security governance needs to address every aspect of an organization. This includes acquisitions, divestitures, and governance committees. Acquisitions and mergers place an organization at an increased level of risk. Such risks include inappropriate information disclosure, data loss, downtime, or failure to achieve sufficient return on investment (ROI).

Similarly, a divestiture or any form of asset or employee reduction is another time period of increased risk and thus increased need for focused security governance. Often, security governance is managed by a governance committee or at least a board of directors. This is the group of influential knowledge experts whose primary task is to oversee and guide the actions of security and operations for an organization. (Stewart et al., 2004)

5. Security Management Concepts and Principles

Security management concepts and principles are inherent elements in a security policy and solution deployment. They define the basic parameters needed for a secure environment. They also define the goals and objectives that both policy designers and system implementers must achieve to create a secure solution. It is important for real-world security professionals to understand these items thoroughly.

The primary goals and objectives of security are contained within the CIA Triad, which is the name given to the three primary security principles:

- Confidentiality
- Integrity
- Availability

Security controls are typically evaluated on how well they address these core information security tenets. Overall, a complete security solution should adequately address each of these tenets. Vulnerabilities and risks are also evaluated based on the threat they pose against one or more of the CIA Triad principles. Thus, it is a good idea to be familiar with these principles and use them as guidelines for judging all things related to security.
These three principles are considered the most important within the realm of security. However important each specific principle is to a specific organization depends on the organization's security goals and requirements and on the extent to which the organization's security might be threatened. (Stewart et al., 2004)

- **Confidentiality**

  The first principle of the CIA Triad is confidentiality. If a security mechanism offers confidentiality, it offers a high level of assurance that data, objects, or resources are restricted from unauthorized subjects. If a threat exists against confidentiality, unauthorized disclosure could take place.

  In general, for confidentiality to be maintained on a network, data must be protected from unauthorized access, use, or disclosure while in storage, in process, and in transit. Unique and specific security controls are required for each of these states of data, resources, and objects to maintain confidentiality.
  Numerous countermeasures can help ensure confidentiality against possible threats. These include encryption, network traffic padding, strict access control, rigorous authentication procedures, data classification, and extensive personnel training.

  Confidentiality and integrity depend on each other. Without object integrity, confidentiality cannot be maintained. (Stewart et al., 2004)

- **Integrity**

  For integrity to be maintained, objects must retain their veracity and be intentionally modified by only authorized subjects. If a security mechanism offers integrity, it offers a high level of assurance that the data, objects, and resources are unaltered from their original protected state. Alterations should not occur while the object is in storage, in transit, or in process. Thus, maintaining integrity means the object itself is not altered and the operating system and programming entities that manage and manipulate the object are not compromised.

  Integrity can be examined from three perspectives:
  - Preventing unauthorized subjects from making modifications;
  - Preventing authorized subjects from making unauthorized modifications, such as mistakes;
  - Maintaining the internal and external consistency of objects so that their data is a correct and true reflection of the real world and any relationship with any child, peer, or parent object is valid, consistent, and verifiable.

  Numerous attacks focus on the violation of integrity. These include viruses, logic bombs, unauthorized access, errors in coding and applications, malicious modification, intentional replacement, and system back doors. (Stewart et al., 2004)

- **Availability**

  The third principle of the CIA Triad is availability, which means authorized subjects are granted timely and uninterrupted access to objects. If a security mechanism offers

availability, it offers a high level of assurance that the data, objects, and resources are accessible to authorized subjects. Availability includes efficient uninterrupted access to objects and prevention of denial of service (DoS) attacks. Availability also implies that the supporting infrastructure-including network services, communications, and access control mechanisms-is functional and allows authorized users to gain authorized access.

For availability to be maintained on a system, controls must be in place to ensure authorized access and an acceptable level of performance, to quickly handle interruptions, to provide for redundancy, to maintain reliable backups, and to prevent data loss or destruction.

Most security policies, as well as business continuity planning (BCP), focus on the use of fault tolerance features at the various levels of access/storage/security (i.e., disk, server, site) with the goal of eliminating single points of failure to maintain availability of critical systems. (Stewart et al., 2004)

6. Data Classification

Data classification, or categorization, is the primary means by which data is protected based on its need for secrecy, sensitivity, or confidentiality. It is inefficient to treat all data the same way when designing and implementing a security system because some data items need more security than others. Securing everything at a low security level means sensitive data is easily accessible. Securing everything at a high security level is too expensive and restricts access to unclassified, noncritical data. Data classification is used to determine how much effort, money, and resources are allocated to protect the data and control access to it. Data classification, or categorization, is the process of organizing items, objects, subjects, and so on into groups, categories, or collections with similarities. These similarities could include value, cost, sensitivity, risk, vulnerability, power, privilege, possible levels of loss or damage, or need to know.

The primary objective of data classification schemes is to formalize and stratify the process of securing data based on assigned labels of importance and sensitivity. Data classification is used to provide security mechanisms for storing, processing, and transferring data. It also addresses how data is removed from a system and destroyed.
The following are some benefits of using a data classification scheme:

- It demonstrates an organization's commitment to protecting valuable resources and assets;
- It assists in identifying those assets that are most critical or valuable to the organization;
- It lends credence to the selection of protection mechanisms;
- It is often required for regulatory compliance or legal restrictions;
- It helps to define access levels, types of authorized uses, and parameters for declassification and/or destruction of resources that are no longer valuable.

The criteria by which data is classified vary based on the organization performing the classification. However, you can glean numerous generalities from common or standardized classification systems:

- Usefulness of the data;
- Timeliness of the data;
- Value or cost of the data;
- Maturity or age of the data;
- Lifetime of the data (or when it expires);
- Association with personnel;
- Data disclosure damage assessment (that is, how the disclosure of the data would affect the organization);
- Data modification damage assessment (that is, how the modification of the data would affect the organization);
- National security implications of the data;
- Authorized access to the data (that is, who has access to the data);
- Restriction from the data (that is, who is restricted from the data);
- Maintenance and monitoring of the data (that is, who should maintain and monitor the data);
- Storage of the data.

Using whatever criteria is appropriate for the organization, data is evaluated, and an appropriate data classification label is assigned to it. (Stewart et al., 2004)

Accountability and Access Control

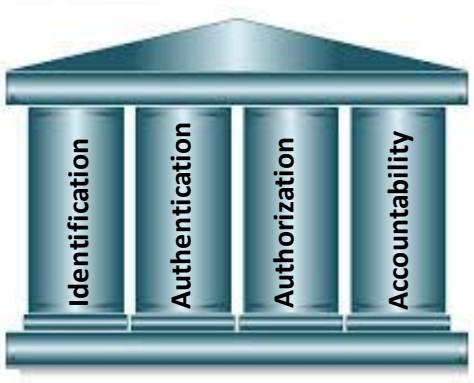
Policies are an important element of access control because they help personnel within the organization understand what security requirements are important. The security policy is created or approved by senior leadership, and it provides a broad overview of an organization's security needs but usually does not go into details about how to fulfill the needs. For example, it may state the need to implement and enforce separation of duties and least privilege principles but not state how to do so. Professionals within the organization use the security policies as a guide to implement security requirements. Standards are also created from security policies (Stewart et al., 2004).

1. Purpose

The purpose of this policy is to protect Lebanese government organizations data by controlling access to IT assets through rules, requirements, and guidelines. The IT assets include, but are not limited to, systems, networks, media, storage, applications, operating systems, and databases. The IT assets should fall under the responsibility of the Office of Information Technology of the organization.
This policy is applicable to all users who have access to the organization data and its IT assets.

2. Introduction

Access Control is the framework for ensuring the safety of IT assets against inadvertent unauthorized access and appropriately controlling IT assets access. The framework is based on four pillars, including *Identification*, *Authentication*, *Authorization* and *Accountability*.



All IT and administrative departments are responsible for developing the relevant Operational Procedures, Working Instructions, and Technical Documents in line with the rules, requirements, and guidelines set forth in this policy.

Identification

Identification is the process by which a subject professes an identity and accountability is initiated. For example, a user provides a username, a logon ID, or a smart card to represent an identification process. Similarly, an application can provide a process ID number as identification. Once a subject has identified itself, the claimed identity becomes accountable for any further actions undertaken by that subject. IT systems track activity by identities, not by subjects themselves. A computer doesn't know one human from another, but it does know that your user account is different from all other user accounts. (Stewart et al., 2004)

All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user. (NL ISO/IEC, 2010)

Authentication

Authentication is the process of verifying or testing that a claimed identity is valid. Authentication requires that a subject provide additional information that must correspond exactly to the professed identity. An authentication system checks the professed identity and the authentication against a database. If the database includes the identity and the correct authentication is included, the subject is authenticated.

The three basic methods of authentication are also known as types or factors.

Type 1: A Type 1 authentication factor is something you know. It is any string of characters you have memorized and can reproduce on a keyboard when prompted. Examples include a password, personal identification number (PIN), passphrase, or mother's maiden name.

Type 2: A Type 2 authentication factor is something you have. It is a physical device that you must have in your possession at the time of authentication. Examples include a token device, smart card, memory card, or USB drive.

Type 3: A Type 3 authentication factor is something you are or something you do. It is a physical characteristic of a person identified with different types of biometrics. Examples in the "something you are" category include fingerprints, voice prints, retina patterns, iris patterns, face shapes, palm topology, and hand geometry. Examples in the "something you do" category include signature and keystroke dynamics, also known as behavioral biometrics. (Stewart et al., 2004)

Authorization

Authorization indicates who is trusted to perform specific operations. If the action is allowed, the subject is authorized; if disallowed, the subject is not authorized.

It's important to realize that just because users or other entities can authenticate to a system, that doesn't mean they are given access to anything and everything. Instead, subjects are authorized access to specific objects based on their proven identity. The process of authorization ensures that the requested activity or object access is possible based on the privileges assigned to the subject. (Stewart et al., 2004)

Accountability

Accountability, which is done via auditing, logging, and monitoring, ensures that subjects can be held accountable for their actions. Auditing is the process of tracking and recording subject activities within logs. Logs typically record who took an action, when and where the action was taken, and what the action was. One or more logs create an audit trail that can be used to reconstruct events and to verify whether a security policy or authorization was violated. When contents of audit trails are reviewed, people associated with the accounts can be held accountable for their actions. Accountability relies on effective identification and authentication, but it does not require effective authorization. In other words, if users are adequately identified and authenticated, accountability mechanisms such as audit logs can track their activity, even when they access resources they shouldn't. (Stewart et al., 2004)

3. User Access Management

3.1. User Registration

There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services. (NL ISO/IEC, 2010)

The access control procedure for user registration and de-registration should be clear and contain all the necessary steps and details in order to comply with the policy procedures.

3.2. Privilege Management

The allocation and use of privileges should be restricted and controlled. Multi-user systems that require protection against unauthorized access should have the allocation of privileges controlled through a formal authorization process.

Inappropriate use of system administration privileges (any feature or facility of an information system that enables the user to override system or application controls) can be a major contributory factor to the failures or breaches of systems. (NL ISO/IEC, 2010)

3.3. User Password Management

The allocation of passwords should be controlled through a formal management process.
The process should include the following requirements:

a) Users should be required to sign a statement to keep personal passwords;
b) confidential and to keep group passwords solely within the members of the group;
c) When users are required to maintain their own passwords they should be provided initially with a secure temporary password, which they are forced to change immediately;
d) Temporary passwords should be given to users in a secure manner;
e) temporary passwords should be unique to an individual and should not be guessable;
f) passwords should never be stored on computer systems in an unprotected form;

Passwords are a common means of verifying a user's identity before access is given to an information system or service according to the user's authorization. Other technologies for user identification and authentication, such as biometrics, e.g. finger-print verification, signature verification, and use of hardware tokens, e.g. smart cards, are available, and should be considered if appropriate. (NL ISO/IEC, 2010)

4. User Responsibilities

To prevent unauthorized user access, and compromise or theft of information and information processing facilities.
The co-operation of authorized users is essential for effective security. (NL ISO/IEC, 2010)

4.1. Password Use

Users should be required to follow good security practices in the selection and use of passwords.
All users should be advised to:

a) keep passwords confidential;
b) avoid keeping a record (e.g. paper, software file or hand-held device) of passwords, unless this can be stored securely and the method of storing has been approved;
c) change passwords whenever there is any indication of possible system or password compromise;
d) select quality passwords with sufficient minimum length which are:
    1) easy to remember;
    2) not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers, and dates of birth etc.;
    3) not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries);
    4) free of consecutive identical, all-numeric or all-alphabetic characters.

> "Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months."
>
> – *Clifford Stoll* – American astronomer, author and teacher

e) change passwords at regular intervals or based on the number of accesses (passwords for privileged accounts should be changed more frequently than normal passwords), and avoid re-using or cycling old passwords;
f) change temporary passwords at the first log-on;
g) not include passwords in any automated log-on process, e.g. stored in a macro or function key;
h) not share individual user passwords;
i) not use the same password for business and non-business purposes.

All users should be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection.

Users should be advised to:

a) terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver;
b) log-off mainframe computers, servers, and office PCs when the session is finished (i.e. not just switch off the PC screen or terminal);
c) secure PCs or terminals from unauthorized use by a key lock or an equivalent control, e.g. password access, when not in use.

(NL ISO/IEC, 2010)

4.2. Password Selection

Passwords can be effective if selected intelligently and managed properly. A password policy can be part of the organization's written policy that dictates the requirements for passwords. Many systems also include technical password policies that enforce the password restriction requirements. Password policies can, for example, ensure that users change their passwords regularly (e.g. a maximum age setting might specify that users must change their password every 45 days). The following list includes some other password policy settings:

***Password length*:** The length is the number of characters in the password. End user passwords should be at least eight characters long, and many organizations require privileged account passwords to be at least 15 characters long. This specifically overcomes a weakness in how passwords are stored in some Windows systems.

***Password complexity*:** The complexity of a password refers to how many character types it includes. An eight-character password using uppercase characters, lowercase characters, symbols, and numbers is much stronger than an eight-character password using only numbers.

***Password history*:** Many users get into the habit of switching between two passwords. A password history remembers a certain number of previous passwords (perhaps six) and prevents users from reusing a password in the history. This is often combined with a

minimum password age setting, preventing users from changing a password repeatedly until they can set the password back to the original one. Minimum password age is often set to one day.

However, even with strong software-enforced password restrictions, it remains possible to create passwords that may be easily guessed or cracked. Users don't always understand the need for strong passwords, or even how to create them. An organization's security policy will usually stress the need for strong passwords and define the contents of a strong password. If end users create their own passwords, suggestions like the following can help them create strong ones:

- Do not use any part of your name, logon name, email address, employee number, Social Security number, phone number, extension, or other identifying name or code;
- Do not use dictionary words (including words in foreign dictionaries), slang, or industry acronyms;
- Do use nonstandard capitalization and spelling;
- Do switch letters and replace letters with numbers.

In some environments, initial passwords for user accounts are generated automatically. Often the generated password is a form of a composition password, which is constructed from two or more unrelated words joined together with a number or symbol in between. Composition passwords are easy for computers to generate, but they should not be used for extended periods of time because they are vulnerable to password-guessing attacks. If the algorithm for computer-generated passwords is discovered, all passwords created by the system are in jeopardy of being compromised. (Stewart et al., 2004)

4.3. Password Phrases

A password mechanism that is more effective than a basic password is a passphrase. A passphrase is a string of characters similar to a password but it has unique meaning to the user. Passphrases are often basic sentences modified to simplify memorization. Here's an example: "I passed the security exam" can be converted to the following passphrase: "IP@$$edTheSecurityEx@m." Using a passphrase has several benefits. It is difficult to crack a passphrase using a brute-force tool, and it encourages the use of a lengthy string with numerous characters, but it is still easy to remember. (Stewart et al., 2004)

4.4. Clear Desk and Clear Screen Policy

A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.

The clear desk and clear screen policy should take into account the information classifications, legal and contractual requirements, and the corresponding risks and cultural aspects of the organization.

A clear desk/clear screen policy reduces the risks of unauthorized access, loss of, and damage to information during and outside normal working hours. Safes or other forms of secure storage facilities might also protect information stored therein against disasters such as a fire, earthquake, flood or explosion. (NL ISO/IEC, 2015)

5. Access Control to Program Source Code

Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) should be strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes as well as to maintain the confidentiality of valuable intellectual property. For program source code, this can be achieved by controlled central storage of such code, preferably in program source libraries.

The following guidelines should then be considered to control access to such program source libraries in order to reduce the potential for corruption of computer programs:

a) where possible, program source libraries should not be held in operational systems;
b) support personnel should not have unrestricted access to program source libraries;
c) the updating of program source libraries and associated items and the issuing of program sources to programmers should only be performed after appropriate authorization has been received;
d) an audit log should be maintained of all accesses to program source libraries;
e) If the program source code is intended to be published, additional controls to help getting assurance on its integrity (e.g. digital signature) should be considered.

(NL ISO/IEC, 2015)

Secure Network Architecture and Network Access Control

The Internet is host to countless information services and numerous applications, including the Web, email, FTP, Telnet, newsgroups, chat, and so on. The Internet is also home to malicious people whose primary goal is to locate your computer and extract valuable data from it, use it to launch further attacks, or damage it in some way. You should be familiar with the Internet and able to readily identify its benefits and drawbacks from your own online experiences. (Stewart et al., 2004)

1. Purpose

Because of the success and global use of the Internet, many of its technologies were adapted or integrated into the private business network. This created two new forms of network segments: intranets and extranets.

An *intranet* is a private network that is designed to host the same information services found on the Internet. Networks that rely upon external servers to provide information services internally are not considered intranets. Intranets provide users with access to the Web, email, and other services on internal servers that are not accessible to anyone outside the private network.

An *extranet* is a cross between the Internet and an intranet. An extranet is a section of an organization's network that has been sectioned off so that it acts as an intranet for the private network but also serves information to the public Internet. An extranet is often reserved for use by specific partners or customers. It is rarely on a public network. An extranet for public consumption is typically labeled a demilitarized zone (DMZ) or perimeter network. (Stewart et al., 2004)

2. Introduction

Networks are not typically configured as one single large collection of systems. Usually networks are segmented or subdivided into smaller organizational units. These smaller units, grouping, segments, or subnetworks (i.e., subnets) can be used to improve various aspects of the network:

Boosting performance Network segmentation can improve performance through an organizational scheme in which systems that often communicate are located in the same segment while systems that rarely or never communicate are located in other segments.

Reducing communication problems Network segmentation often reduces congestion and contains communication problems, such as broadcast storms, to individual subsections of the network.

Providing security Network segmentation can also improve security by isolating traffic and user access to those segments where they are authorized.

Segments can be created by using switch-based VLANs, routers, or firewalls, individually or in combination. A private LAN or intranet, a DMZ, and an extranet are all types of network segments.

When you're designing a secure network (whether a private network, an intranet, or an extranet), you must evaluate numerous networking devices. Not all of these components are necessary for a secure network, but they are all common network devices that may have an impact on network security. (Stewart et al., 2004)

3. Network and Protocol Security Mechanisms

TCP/IP is the primary protocol suite used on most networks and on the Internet. It is a robust protocol suite, but it has numerous security deficiencies. In an effort to improve the security of TCP/IP, many sub-protocols, mechanisms, or applications have been developed to protect the confidentiality, integrity, and availability of transmitted data.

It is important to remember that even with the foundational protocol suite of TCP/IP; there are literally hundreds, if not thousands, of individual protocols, mechanisms, and applications in use across the Internet. Some of them are designed to provide security services. Some protect integrity, others protect confidentiality, and others provide authentication and access control. (Stewart et al., 2004)

4. Network Access Control

Controlling network access is to prevent unauthorized access to networked services. Access to both internal and external networked services should be controlled. User access to networks and network services should not compromise the security of the network services by ensuring:

a) appropriate interfaces are in place between the organization's network and networks owned by other organizations, and public networks;
b) appropriate authentication mechanisms are applied for users and equipment;
c) control of user access to information services is enforced.

(NL ISO/IEC, 2010)

4.1. Policy on Use of Network Services

Users should only be provided with access to the services that they have been specifically authorized to use.

A policy should be formulated concerning the use of networks and network services. This policy should cover:

a) the networks and network services which are allowed to be accessed;
b) authorization procedures for determining who is allowed to access which networks and networked services;
c) management controls and procedures to protect access to network connections and network services;
d) the means used to access networks and network services (e.g. the conditions for allowing dial-up access to an Internet service provider or remote system).

Unauthorized and insecure connections to network services can affect the whole organization. This control is particularly important for network connections to sensitive or critical business applications or to users in high-risk locations. (NL ISO/IEC, 2010)

4.2. Segregation in Networks

One method of managing the security of large networks is to divide them into separate network domains.

The domains can be chosen based on trust levels (e.g. public access domain, desktop domain, server domain), along organizational units (e.g. human resources, finance, marketing) or some combination (e.g. server domain connecting to multiple organizational units). The segregation can be done using either physically different networks or by using different logical networks (e.g. virtual private networking).

The perimeter of each domain should be well defined. Access between network domains is allowed, but should be controlled at the perimeter using a gateway (e.g. firewall, filtering router). The criteria for segregation of networks into domains, and the access allowed through the gateways, should be based on an assessment of the security requirements of each domain. The assessment should be in accordance with the access control policy, access requirements, value and classification of information processed and also take account of the relative cost and performance impact of incorporating suitable gateway technology.

Wireless networks require special treatment due to the poorly defined network perimeter. For sensitive environments, consideration should be made to treat all wireless access as external connections and to segregate this access from internal networks until the access has passed

through a gateway in accordance with network controls policy before granting access to internal systems.

The authentication, encryption and user level network access control technologies of modern, standards based wireless networks may be sufficient for direct connection to the organization's internal network when properly implemented.

Networks often extend beyond organizational boundaries, as business partnerships are formed that require the interconnection or sharing of information processing and networking facilities. Such extensions can increase the risk of unauthorized access to the organization's information systems that use the network, some of which require protection from other network users because of their sensitivity or criticality. (NL ISO/IEC, 2015)

4.3. Security of Network Services

Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.

The ability of the network service provider to manage agreed services in a secure way should be determined and regularly monitored, and the right to audit should be agreed.
The security arrangements necessary for particular services, such as security features, service levels and management requirements, should be identified. The organization should ensure that network service providers implement these measures.

Network services include the provision of connections, private network services and value added networks and managed network security solutions such as firewalls and intrusion detection systems.

These services can range from simple unmanaged bandwidth to complex value-added offerings.

Security features of network services could be:

a) technology applied for security of network services, such as authentication, encryption and network connection controls;
b) technical parameters required for secured connection with the network services in accordance with the security and network connection rules;
c) procedures for the network service usage to restrict access to network services or applications, where necessary.

(NL ISO/IEC, 2010)

4.4. Electronic Messaging

Information involved in electronic messaging should be appropriately protected.

Information security considerations for electronic messaging should include the following:

a) protecting messages from unauthorized access, modification or denial of service commensurate with the classification scheme adopted by the organization;
b) ensuring correct addressing and transportation of the message;
c) reliability and availability of the service;
d) legal considerations, for example requirements for electronic signatures;
e) obtaining approval prior to using external public services such as instant messaging, social networking or file sharing;
f) stronger levels of authentication controlling access from publicly accessible networks.

There are many types of electronic messaging such as email, electronic data interchange and social networking which play a role in business communications. (NL ISO/IEC, 2015)

5. Mobile Device Policy

Mobile devices include smartphones and tablets. These devices have internal memory or removable memory cards that can hold a significant amount of data. Data can include email with attachments, contacts, and scheduling information. Additionally, many devices include applications that allow users to read and manipulate different types of documents.

> "App stores and mobile apps are the greatest hostile code and malware delivery mechanism ever created."
>
> – *Winn Schwartau* – Chairman of mobileactivedefense.com

Organizations often purchase smartphones for users and maintain their data plans. This is certainly a great benefit for the employee, but it also gives the organization additional control over the user's phone and the data it contains. Some of the common controls organizations enable on user phones are encryption, screen lock, Global Positioning System (GPS), and remote wipe. Encryption protects the data if the phone is lost or stolen, the screen lock slows down someone that may have stolen a phone, and GPS provides information on the location of the phone if it is lost or stolen. A remote wipe signal can be sent to a lost device to delete all data on the device if it has been lost and includes valuable data. Many devices respond with a confirmation message when the remote wipe has succeeded. (Stewart et al., 2004)

A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices. When using mobile devices, special care should be taken to ensure that business information is not compromised. The mobile device policy should take into account the risks of working with mobile devices in unprotected environments.

The mobile device policy should consider:

a) registration of mobile devices;
b) requirements for physical protection;

c) restriction of software installation;
d) requirements for mobile device software versions and for applying patches;
e) restriction of connection to information services;
f) access controls;
g) cryptographic techniques;
h) malware protection;
i) remote disabling, erasure or lockout;
j) backups;
k) usage of web services and web apps.

Mobile devices should also be physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centers and meeting places. Devices carrying important, sensitive or critical business information should not be left unattended and, where possible, should be physically locked away, or special locks should be used to secure the devices.

Where the mobile device policy allows the use of privately owned mobile devices, the policy and related security measures should also consider:

a) separation of private and business use of the devices, including using software to support such separation and protect business data on a private device;
b) providing access to business information only after users have signed an end user agreement acknowledging their duties (physical protection, software updating, etc.), waiving ownership of business data, allowing remote wiping of data by the organization in case of theft or loss of the device or when no longer authorized to use the service. This policy needs to take account of privacy legislation.

(NL ISO/IEC, 2015)

6. Information Transfer Policies and Procedures

Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities.

The procedures and controls to be followed when using communication facilities for information transfer should consider the following items:

a) procedures designed to protect transferred information from interception, copying, modification, miss-routing and destruction;
b) procedures for the detection of and protection against malware that may be transmitted through the use of electronic communications;
c) procedures for protecting communicated sensitive electronic information that is in the form of an attachment;
d) policy or guidelines outlining acceptable use of communication facilities;
e) use of cryptographic techniques e.g. to protect the confidentiality, integrity and authenticity of information;

f) controls and restrictions associated with using communication facilities, e.g. automatic forwarding of electronic mail to external mail addresses;
g) advising personnel to take appropriate precautions not to reveal confidential information.

In addition, personnel should be reminded that they should not have confidential conversations in public places or over insecure communication channels, open offices and meeting places.

Information transfer services should comply with any relevant legal requirements. Information transfer may occur through the use of a number of different types of communication facilities, including electronic mail, voice, facsimile and video.

Software transfer may occur through a number of different mediums, including downloading from the Internet and acquisition from vendors selling off-the-shelf products.

The business, legal and security implications associated with electronic data interchange, electronic commerce and electronic communications and the requirements for controls should be considered. (NL ISO/IEC, 2015)

6.1. Agreements on Information Transfer

Agreements should address the secure transfer of business information between the organization and external parties.

Information transfer agreements should incorporate the following:

a) management responsibilities for controlling and notifying transmission, dispatch and receipt;
b) procedures to ensure traceability and non-repudiation;
c) minimum technical standards for packaging and transmission;
d) courier identification standards;
e) responsibilities and liabilities in the event of information security incidents, such as loss of data;
f) use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected;
g) technical standards for recording and reading information and software;
h) any special controls that are required to protect sensitive items, such as cryptography;
i) maintaining a chain of custody for information while in transit;
j) acceptable levels of access control.

Policies, procedures and standards should be established and maintained to protect information and physical media in transit, and should be referenced in such transfer agreements.

The information security content of any agreement should reflect the sensitivity of the business information involved.

Agreements may be electronic or manual, and may take the form of formal contracts. For confidential information, the specific mechanisms used for the transfer of such information should be consistent for all organizations and types of agreements. (NL ISO/IEC, 2015)

Physical and Environmental Security

1. Purpose

The purpose of physical security is to protect against physical threats. The following physical threats are among the most common: fire and smoke, water (rising/falling), earth movement (earthquakes, landslides, volcanoes), storms (wind, lightning, rain, snow, sleet, ice), sabotage/vandalism, explosion/destruction, building collapse, toxic materials, utility loss (power, heating, cooling, air, water), equipment failure, theft, and personnel loss (strikes, illness, access, transport).
In many cases, you'll need a disaster recovery plan or a business continuity plan should a serious physical threat (such as an explosion, sabotage, or natural disaster) occur (Stewart et al., 2004).

2. Introduction

Most people think about locks, bars, alarms, and uniformed guards when they think about security. While these countermeasures are by no means the only precautions that need to be considered when trying to secure an information system, they are a perfectly logical place to begin. Physical security is a vital part of any security plan and is fundamental to all security efforts--without it, information security, software security, user access security, and network security are considerably more difficult, if not impossible, to initiate. Physical security refers to the protection of building sites and equipment (and all information and software contained therein) from theft, vandalism, natural disaster, manmade catastrophes, and accidental damage (e.g., from electrical surges, extreme temperatures, and spilled coffee). It requires solid building construction, suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders (National Center for Education Statistics, 1998).

3. Secure areas

The objective is to prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities. (NL ISO/IEC, 2015)

The design and configuration of internal security, including work areas and visitor areas, should be considered carefully. There should not be equal access to all locations within a facility. Areas that contain assets of higher value or importance should have more restricted access. Valuable and confidential assets should be located in the heart or center of protection provided by a facility. In effect, you should focus

on deploying concentric circles of physical protection. This type of configuration requires increased levels of authorization to gain access into more sensitive areas inside the facility. (Stewart et al., 2004)

4. Physical security perimeter

Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.

The following guidelines should be considered and implemented where appropriate for physical security perimeters:

a) security perimeters should be defined, and the siting and strength of each of the perimeters should depend on the security requirements of the assets within the perimeter and the results of a risk assessment;
b) perimeters of a building or site containing information processing facilities should be physically sound; the exterior roof, walls and flooring of the site should be of solid construction and all external doors should be suitably protected against unauthorized access with control mechanisms, (e.g. bars, alarms, locks); doors and windows should be locked when unattended and external protection should be considered for windows, particularly at ground level;
c) a manned reception area or other means to control physical access to the site or building should be in place; access to sites and buildings should be restricted to authorized personnel only;
d) physical barriers should, where applicable, be built to prevent unauthorized physical access and environmental contamination;
e) all fire doors on a security perimeter should be alarmed, monitored and tested in conjunction with the walls to establish the required level of resistance in accordance with suitable regional, national and international standards; they should operate in accordance with the local fire code in a failsafe manner;
f) suitable intruder detection systems should be installed to national, regional or international standards and regularly tested to cover all external doors and accessible windows; unoccupied areas should be alarmed at all times; cover should also be provided for other areas, e.g. computer room or communications rooms;
g) information processing facilities managed by the organization should be physically separated from those managed by external parties.

Physical protection can be achieved by creating one or more physical barriers around the organization's premises and information processing facilities. The use of multiple barriers gives additional protection, where the failure of a single barrier does not mean that security is immediately compromised.

A secure area may be a lockable office or several rooms surrounded by a continuous internal physical security barrier. Additional barriers and perimeters to control physical access may be needed between areas with different security requirements inside the security perimeter.

Special attention to physical access security should be given in the case of buildings holding assets for multiple organizations.

The application of physical controls, especially for the secure areas, should be adapted to the technical and economic circumstances of the organization, as set forth in the risk assessment. (NL ISO/IEC, 2015)

5. Physical Entry Controls

Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

The following guidelines should be considered:

a) the date and time of entry and departure of visitors should be recorded, and all visitors should be supervised unless their access has been previously approved; they should only be granted access for specific, authorized purposes and should be issued with instructions on the security requirements of the area and on emergency procedures;
b) access to areas where confidential information is processed or stored should be restricted to authorized individuals only by implementing appropriate access controls, e.g. by implementing a two-factor authentication mechanism such as an access card and secret PIN;
c) a physical log book or electronic audit trail of all access should be securely maintained and monitored;
d) all employees, contractors and external parties should be required to wear some form of visible identification and should immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification;
e) external party support service personnel should be granted restricted access to secure areas or confidential information processing facilities only when required; this access should be authorized and monitored;
f) access rights to secure areas should be regularly reviewed and updated, and revoked when necessary.

(NL ISO/IEC, 2015)

6. Securing Offices, Rooms and Facilities

Physical security for offices, rooms and facilities should be designed and applied.

The following guidelines should be considered to secure offices, rooms and facilities:

a) key facilities should be sited to avoid access by the public;
b) where applicable, buildings should be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building, identifying the presence of information processing activities;

c) facilities should be configured to prevent confidential information or activities from being visible and audible from the outside;
d) directories and internal telephone books identifying locations of confidential information processing facilities should not be readily accessible to anyone unauthorized.

(NL ISO/IEC, 2015)

7. Server Rooms and Data Center Security

Server rooms, data centers, communications rooms, wiring closets, server vaults, and IT closets are enclosed, restricted, and protected rooms where your mission-critical servers and network devices are housed. Centralized server rooms need not be human compatible. In fact, the more human incompatible a server room is, the more protection it will offer against casual and determined attacks. Human incompatibility can be accomplished by including Halotron, PyroGen, or other halon-substitute oxygen-displacement fire detection and extinguishing systems, low temperatures, little or no lighting, and equipment stacked with little room to maneuver. Server rooms should be designed to support optimal operation of the IT infrastructure and to block unauthorized human access or intervention.

Server rooms should be located at the core of the building. Try to avoid locating these rooms on the ground floor, the top floor, and the basement whenever possible. Additionally, the server room should be located away from water, gas, and sewage lines. These pose too large a risk of leakage or flooding, which can cause serious damage and downtime. (Stewart et al., 2004)

8. Protecting Against External and Environmental Threats

Physical protection against natural disasters, malicious attack or accidents should be designed and applied.

Specialist advice should be obtained on how to avoid damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster. (NL ISO/IEC, 2015)

9. Working in Secure Areas

Procedures for working in secure areas should be designed and applied.

The following guidelines should be considered:

a) personnel should only be aware of the existence of, or activities within, a secure area on a need-to-know basis;
b) unsupervised working in secure areas should be avoided both for safety reasons and to prevent opportunities for malicious activities;
c) vacant secure areas should be physically locked and periodically reviewed;
d) photographic, video, audio or other recording equipment, such as cameras in mobile devices, should not be allowed, unless authorized.

The arrangements for working in secure areas include controls for the employees and external party users working in the secure area and they cover all activities taking place in the secure area. (NL ISO/IEC, 2015)

10. Delivery and Loading Areas

Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

The following guidelines should be considered:

a) access to a delivery and loading area from outside of the building should be restricted to identified and authorized personnel;
b) the delivery and loading area should be designed so that supplies can be loaded and unloaded without delivery personnel gaining access to other parts of the building;
c) the external doors of a delivery and loading area should be secured when the internal doors are opened;
d) incoming material should be inspected and examined for explosives, chemicals or other hazardous materials, before it is moved from a delivery and loading area;
e) incoming material should be registered in accordance with asset management procedures on entry to the site;
f) incoming and outgoing shipments should be physically segregated, where possible;
g) incoming material should be inspected for evidence of tampering en route. If such tampering is discovered it should be immediately reported to security personnel.

(NL ISO/IEC, 2015)

11. Equipment

To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

11.1. Equipment Siting and Protection

Equipment should be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

The following guidelines should be considered to protect equipment:

a) equipment should be sited to minimize unnecessary access into work areas;
b) information processing facilities handling sensitive data should be positioned carefully to reduce the risk of information being viewed by unauthorized persons during their use;
c) storage facilities should be secured to avoid unauthorized access;
d) items requiring special protection should be safeguarded to reduce the general level of protection required;

e) controls should be adopted to minimize the risk of potential physical and environmental threats, e.g. theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation and vandalism;
f) guidelines for eating, drinking and smoking in proximity to information processing facilities should be established;
g) environmental conditions, such as temperature and humidity, should be monitored for conditions which could adversely affect the operation of information processing facilities;
h) lightning protection should be applied to all buildings and lightning protection filters should be fitted to all incoming power and communications lines;
i) equipment processing confidential information should be protected to minimize the risk of information leakage due to electromagnetic emanation.

(NL ISO/IEC, 2015)

11.2. Supporting Utilities

Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.

Supporting utilities (e.g. electricity, telecommunications, water supply, gas, sewage, ventilation and air conditioning) should:

a) conform to equipment manufacturer's specifications and local legal requirements;
b) be appraised regularly for their capacity to meet business growth and interactions with other supporting utilities;
c) be inspected and tested regularly to ensure their proper functioning;
d) if necessary, be alarmed to detect malfunctions;
e) if necessary, have multiple feeds with diverse physical routing.

Emergency lighting and communications should be provided. Emergency switches and valves to cut off power, water, gas or other utilities should be located near emergency exits or equipment rooms.

Additional redundancy for network connectivity can be obtained by means of multiple routes from more than one utility provider. (NL ISO/IEC, 2015)

11.3. Cabling Security

Power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference or damage.

The following guidelines for cabling security should be considered:

a) power and telecommunications lines into information processing facilities should be underground, where possible, or subject to adequate alternative protection;
b) power cables should be segregated from communications cables to prevent interference;
c) for sensitive or critical systems further controls to consider include:
    1) installation of armored conduit and locked rooms or boxes at inspection and termination points;
    2) use of electromagnetic shielding to protect the cables;
    3) initiation of technical sweeps and physical inspections for unauthorized devices being attached to the cables;
    4) controlled access to patch panels and cable rooms.

(NL ISO/IEC, 2015)

11.4. Equipment Maintenance

Equipment should be correctly maintained to ensure its continued availability and integrity.

The following guidelines for equipment maintenance should be considered:

a) equipment should be maintained in accordance with the supplier's recommended service intervals and specifications;
b) only authorized maintenance personnel should carry out repairs and service equipment;
c) records should be kept of all suspected or actual faults, and of all preventive and corrective maintenance;
d) appropriate controls should be implemented when equipment is scheduled for maintenance, taking into account whether this maintenance is performed by personnel on site or external to the organization; where necessary, confidential information should be cleared from the equipment or the maintenance personnel should be sufficiently cleared;
e) all maintenance requirements imposed by insurance policies should be complied with;
f) before putting equipment back into operation after its maintenance, it should be inspected to ensure that the equipment has not been tampered with and does not malfunction.

(NL ISO/IEC, 2015)

11.5. Removal of Assets

Equipment, information or software should not be taken off-site without prior authorization.

The following guidelines should be considered:

a) employees and external party users who have authority to permit off-site removal of assets should be identified;
b) time limits for asset removal should be set and returns verified for compliance;

c) where necessary and appropriate, assets should be recorded as being removed off-site and recorded when returned;
d) the identity, role and affiliation of anyone who handles or uses assets should be documented and this documentation returned with the equipment, information or software.

Spot checks, undertaken to detect unauthorized removal of assets, can also be performed to detect unauthorized recording devices, weapons, etc., and to prevent their entry into and exit from, the site. Such spot checks should be carried out in accordance with relevant legislation and regulations.

Individuals should be made aware that spot checks are carried out, and the verifications should only be performed with authorization appropriate for the legal and regulatory requirements. (NL ISO/IEC, 2015)

11.6. Security of Equipment and Assets Off-Premises

Security should be applied to off-site assets taking into account the different risks of working outside the organization's premises.

The use of any information storing and processing equipment outside the organization's premises should be authorized by management. This applies to equipment owned by the organization and that equipment owned privately and used on behalf of the organization.

The following guidelines should be considered for the protection of off-site equipment:

a) equipment and media taken off premises should not be left unattended in public places;
b) manufacturers' instructions for protecting equipment should be observed at all times, e.g. protection against exposure to strong electromagnetic fields;
c) controls for off-premises locations, such as home-working, teleworking and temporary sites should be determined by a risk assessment and suitable controls applied as appropriate, e.g. lockable filing cabinets, clear desk policy, access controls for computers and secure communication with the office;
d) when off-premises equipment is transferred among different individuals or external parties, a log should be maintained that defines the chain of custody for the equipment including at least names and organizations of those who are responsible for the equipment.

Risks, e.g. of damage, theft or eavesdropping, may vary considerably between locations and should be taken into account in determining the most appropriate controls.

Information storing and processing equipment includes all forms of personal computers, organizers, mobile phones, smart cards, paper or other form, which is held for home working or being transported away from the normal work location.

It may be appropriate to avoid the risk by discouraging certain employees from working off-site or by restricting their use of portable IT equipment. (NL ISO/IEC, 2015)

11.7. Secure Disposal or Re-use of Equipment

All items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

Equipment should be verified to ensure whether or not storage media is contained prior to disposal or re-use.

Storage media containing confidential or copyrighted information should be physically destroyed or the information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function.

Damaged equipment containing storage media may require a risk assessment to determine whether the items should be physically destroyed rather than sent for repair or discarded. Information can be compromised through careless disposal or re-use of equipment.

In addition to secure disk erasure, whole-disk encryption reduces the risk of disclosure of confidential information when equipment is disposed of or redeployed, provided that:

a) the encryption process is sufficiently strong and covers the entire disk (including slack space, swap files, etc.);
b) the encryption keys are long enough to resist brute force attacks;
c) the encryption keys are themselves kept confidential (e.g. never stored on the same disk).

Techniques for securely overwriting storage media differ according to the storage media technology. Overwriting tools should be reviewed to make sure that they are applicable to the technology of the storage media. (NL ISO/IEC, 2015)

11.8. Unattended User Equipment

Users should ensure that unattended equipment has appropriate protection.

All users should be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection. Users should be advised to:

a) terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver;
b) log-off from applications or network services when no longer needed;
c) secure computers or mobile devices from unauthorized use by a key lock or an equivalent control, e.g. password access, when not in use.

(NL ISO/IEC, 2015)

11.9. Clear Desk and Clear Screen Policy

A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.

The clear desk and clear screen policy should take into account the information classifications, legal and contractual requirements and the corresponding risks and cultural aspects of the organization. The following guidelines should be considered:

a) sensitive or critical business information, e.g. on paper or on electronic storage media, should be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated;
b) computers and terminals should be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism when unattended and should be protected by key locks, passwords or other controls when not in use;
c) unauthorised use of photocopiers and other reproduction technology (e.g. scanners, digital cameras) should be prevented;
d) media containing sensitive or classified information should be removed from printers immediately.

A clear desk/clear screen policy reduces the risks of unauthorized access, loss of and damage to information during and outside normal working hours. Safes or other forms of secure storage facilities might also protect information stored therein against disasters such as a fire, earthquake, flood or explosion.

Consider the use of printers with PIN code function, so the originators are the only ones who can get their print-outs and only when standing next to the printer. (NL ISO/IEC, 2015)

12. Management of Removable Media

Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.

The following guidelines for the management of removable media should be considered:

a) if no longer required, the contents of any re-usable media that are to be removed from the organization should be made unrecoverable;
b) where necessary and practical, authorization should be required for media removed from the organization and a record of such removals should be kept in order to maintain an audit trail;
c) all media should be stored in a safe, secure environment, in accordance with manufacturers' specifications;
d) if data confidentiality or integrity are important considerations, cryptographic techniques should be used to protect data on removable media;
e) to mitigate the risk of media degrading while stored data are still needed, the data should be transferred to fresh media before becoming unreadable;
f) multiple copies of valuable data should be stored on separate media to further reduce the risk of coincidental data damage or loss;
g) registration of removable media should be considered to limit the opportunity for data loss;
h) removable media drives should only be enabled if there is a business reason for doing so;
i) where there is a need to use removable media the transfer of information to such media should be monitored;
j) Procedures and authorization levels should be documented.

(NL ISO/IEC, 2015)

Operations Security and Business continuity

1. Purpose

The primary purpose for security operations practices is to safeguard information assets that reside in a system on a day-to-day basis, to identify and safeguard any vulnerability that might be present in the system, and to prevent any exploitation of threats. This is to ensure correct and secure operations of information processing facilities.
Business continuity planning focuses on maintaining business operations with reduced or restricted infrastructure capabilities or resources. As long as the continuity of the organization's ability to perform its mission-critical work tasks is maintained, BCP can be used to manage and restore the environment. If the continuity is broken, then business processes have stopped and the organization is in disaster mode (Stewart et al., 2004).

> "Make 'Business Continuity' 'Business as Usual' and imbed it into your management routines as decisions are made, instead of an afterthought check off the box exercise later."
>
> *– Bobbie Garrett –*

2. Introduction

The Security Operations domain is focused on identifying and protecting critical information within an organization. There are several core security operations concepts that any organization needs to implement to provide basic security protection. Resource protection ensures that media and other assets that are valuable to an organization are protected throughout the lifetime of the resource.

Patch and vulnerability management controls ensure that systems are kept up-to-date and protected against known vulnerabilities. Configuration management helps ensure that systems are configured similarly, and change management protects against outages from unauthorized changes. Security audits of these controls provide assurances that the controls are in place and providing the desired protections.

Whereas, Business continuity planning involves assessing the risks to organizational processes and creating policies, plans, and procedures to minimize the impact those risks might have on the organization if they were to occur. Business continuity planning is used to maintain the continuous operation of a business in the event of an emergency situation.

The goal of business continuity planners is to implement a combination of policies, procedures, and processes such that a potentially disruptive event has as little impact on the business as possible (Stewart et al., 2004).

3. Documented Operating Procedures

Operating procedures should be documented and made available to all users who need them.

Documented procedures should be prepared for operational activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, backup, equipment maintenance, media handling, computer room and mail handling management and safety.

The operating procedures should specify the operational instructions, including:

a) the installation and configuration of systems;
b) processing and handling of information both automated and manual;
c) backup;
d) scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times;
e) instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities;
f) support and escalation contacts including external support contacts in the event of unexpected operational or technical difficulties;
g) special output and media handling instructions, such as the use of special stationery or the management of confidential output including procedures for secure disposal of output from failed jobs;
h) system restart and recovery procedures for use in the event of system failure;
i) the management of audit-trail and system log information;
j) monitoring procedures.

Operating procedures and the documented procedures for system activities should be treated as formal documents and changes authorized by management. Where technically feasible, information systems should be managed consistently, using the same procedures, tools and utilities. (NL ISO/IEC, 2015)

4. Patch and Vulnerability Management

Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

Patch management and vulnerability management work together to help protect an organization against emerging threats. Bugs and security vulnerabilities are routinely discovered in operating systems and applications. As they are discovered, vendors write and test patches to remove the vulnerability. Patch management ensures that appropriate patches are applied and vulnerability management helps verify that systems are not vulnerable to known threats.

Patch is a blanket term for any type of code written to correct a bug or vulnerability or improve the performance of existing software. The software can be either an operating system or an application. Patches are sometimes referred to as updates, quick fixes, and hot fixes. In the context of security, the patches that administrators are primarily concern with are patches that affect the vulnerability of a system. These are often referred to as security patches. Service packs are collections of patches that bring a system up-to-date with current patches.

Even though vendors regularly write and release patches, these patches are useful only if they are applied. This may seem obvious, but many security incidents could have been completely avoided if systems were patched. An effective patch management program ensures that systems are kept up-to-date with current patches. These are the common steps within an effective patch management program:

Evaluate patches: When patches are released, administrators evaluate the patch to determine if it applies to their systems.

Test patches: Whenever possible, patches are tested on an isolated system to determine if they have any unwanted side effects. The worst case scenario is that a system will no longer start after a patch is applied.

Approve the patches: Once patches have been tested and are determined to be safe, they are approved for deployment.

Deploy the patches: After testing and approval, patches are deployed to systems. Many organizations use automated methods to deploy the patches.

Verify that patches are deployed: After patches are deployed, systems are regularly audited and tested to ensure that they are patched.
(Stewart et al., 2004)

5. Capacity Management

The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

Capacity requirements should be identified, taking into account the business criticality of the concerned system. System tuning and monitoring should be applied to ensure and, where

necessary, improve the availability and efficiency of systems. Detective controls should be put in place to indicate problems in due time. Projections of future capacity requirements should take account of new business and system requirements and current and projected trends in the organization's information processing capabilities.

Particular attention needs to be paid to any resources with long procurement lead times or high costs; therefore managers should monitor the utilization of key system resources. They should identify trends in usage, particularly in relation to business applications or information systems management tools.

Managers should use this information to identify and avoid potential bottlenecks and dependence on key personnel that might present a threat to system security or services, and plan appropriate action.

Providing sufficient capacity can be achieved by increasing capacity or by reducing demand.

Examples of managing capacity demand include:

a) deletion of obsolete data (disk space);
b) decommissioning of applications, systems, databases or environments;
c) optimising batch processes and schedules;
d) optimising application logic or database queries;
e) denying or restricting bandwidth for resource-hungry services if these are not business critical (e.g. video streaming).

A documented capacity management plan should be considered for mission critical systems.

This control also addresses the capacity of the human resources, as well as offices and facilities. (NL ISO/IEC, 2015)

6. Separation of Development, Testing and Operational Environments

Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment.

The level of separation between operational, testing, and development environments that is necessary to prevent operational problems should be identified and implemented.

The following items should be considered:

a) rules for the transfer of software from development to operational status should be defined and documented;
b) development and operational software should run on different systems or computer processors and in different domains or directories;
c) changes to operational systems and applications should be tested in a testing or staging environment prior to being applied to operational systems;

d) other than in exceptional circumstances, testing should not be done on operational systems;
e) compilers, editors and other development tools or system utilities should not be accessible from operational systems when not required;
f) users should use different user profiles for operational and testing systems, and menus should display appropriate identification messages to reduce the risk of error;
g) sensitive data should not be copied into the testing system environment unless equivalent controls are provided for the testing system.

Development and testing activities can cause serious problems, e.g. unwanted modification of files or system environment or system failure. There is a need to maintain a known and stable environment in which to perform meaningful testing and to prevent inappropriate developer access to the operational environment.

Development and testing personnel also pose a threat to the confidentiality of operational information. Development and testing activities may cause unintended changes to software or information if they share the same computing environment. Separating development, testing and operational environments is therefore desirable to reduce the risk of accidental change or unauthorized access to operational software and business data. (NL ISO/IEC, 2015)

7. Information Backup

Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy.

A backup policy should be established to define the organization's requirements for backup of information, software and systems.

The backup policy should define the retention and protection requirements.

"Being too busy to worry about backup is like being too busy driving a car to put on a seatbelt."

– T.E. Ronneberg– Writer, and web developer from Sydney, Australia

Adequate backup facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.

When designing a backup plan, the following items should be taken into consideration:

a) accurate and complete records of the backup copies and documented restoration procedures should be produced;
b) the extent (e.g. full or differential backup) and frequency of backups should reflect the business requirements of the organization, the security requirements of the information involved and the criticality of the information to the continued operation of the organization;

c) the backups should be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site;
d) backup information should be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site;
e) backup media should be regularly tested to ensure that they can be relied upon for emergency use when necessary; this should be combined with a test of the restoration procedures and checked against the restoration time required. Testing the ability to restore backed-up data should be performed onto dedicated test media, not by overwriting the original media in case the backup or restoration process fails and causes irreparable data damage or loss;
f) in situations where confidentiality is of importance, backups should be protected by means of encryption.

Operational procedures should monitor the execution of backups and address failures of scheduled backups to ensure completeness of backups according to the backup policy.

Backup arrangements for individual systems and services should be regularly tested to ensure that they meet the requirements of business continuity plans. In the case of critical systems and services, backup arrangements should cover all systems information, applications and data necessary to recover the complete system in the event of a disaster.

The retention period for essential business information should be determined, taking into account any requirement for archive copies to be permanently retained. (NL ISO/IEC, 2015)

8. Logging and Monitoring

Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed.

Event logs should include, when relevant:

a) user IDs;
b) system activities;
c) dates, times and details of key events, e.g. log-on and log-off;
d) device identity or location if possible and system identifier;
e) records of successful and rejected system access attempts;
f) records of successful and rejected data and other resource access attempts;
g) changes to system configuration;
h) use of privileges;
i) use of system utilities and applications;
j) files accessed and the kind of access;
k) network addresses and protocols;
l) alarms raised by the access control system;
m) activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems;

n) records of transactions executed by users in applications.

Event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security.

Event logs can contain sensitive data and personally identifiable information. Appropriate privacy protection measures should be taken.

Where possible, system administrators should not have permission to erase or de-activate logs of their own activities. (NL ISO/IEC, 2015)

9. Securing Application Services on Public Networks

Information involved in application services passing over public networks should be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

Information security considerations for application services passing over public networks should include the following:

a) the level of confidence each party requires in each other's claimed identity, e.g. through authentication;
b) authorization processes associated with who may approve contents of, issue or sign key transactional documents;
c) ensuring that communicating partners are fully informed of their authorizations for provision or use of the service;
d) determining and meeting requirements for confidentiality, integrity, proof of dispatch and receipt of key;
e) documents and the non-repudiation of contracts, e.g. associated with tendering and contract processes;
f) the level of trust required in the integrity of key documents;
g) the protection requirements of any confidential information;
h) the confidentiality and integrity of any order transactions, payment information, delivery address details and confirmation of receipts;
i) the degree of verification appropriate to verify payment information supplied by a customer;
j) selecting the most appropriate settlement form of payment to guard against fraud;
k) the level of protection required to maintain the confidentiality and integrity of order information;
l) avoidance of loss or duplication of transaction information;
m) liability associated with any fraudulent transactions;
n) insurance requirements.

Many of the above considerations can be addressed by the application of cryptographic controls, taking into account compliance with legal requirements.

Applications accessible via public networks are subject to a range of network related threats, such as fraudulent activities, contract disputes or disclosure of information to the public. Therefore, detailed risk assessments and proper selection of controls are indispensable. Controls required often include cryptographic methods for authentication and securing data transfer.

Application services can make use of secure authentication methods, e.g. using public key cryptography and digital signatures to reduce the risks. Also, trusted third parties can be used, where such services are needed. (NL ISO/IEC, 2015)

10. Protecting Application Services Transactions

Information involved in application service transactions should be protected to prevent incomplete transmission, miss-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

Information security considerations for application service transactions should include the following:

a) the use of electronic signatures by each of the parties involved in the transaction;
b) all aspects of the transaction, i.e. ensuring that:
    1) user's secret authentication information of all parties are valid and verified;
    2) the transaction remains confidential;
    3) privacy associated with all parties involved is retained;
c) communications path between all involved parties is encrypted;
d) protocols used to communicate between all involved parties are secured;
e) ensuring that the storage of the transaction details is located outside of any publicly accessible environment, e.g. on a storage platform existing on the organizational intranet, and not retained and exposed on a storage medium directly accessible from the Internet;
f) where a trusted authority is used (e.g. for the purposes of issuing and maintaining digital signatures or digital certificates) security is integrated and embedded throughout the entire end-to-end certificate/signature management process.

(NL ISO/IEC, 2015)

11. Planning Information Security Continuity

The information security continuity should be embedded in the organization's business continuity management systems.

The organization should determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.

An organization should determine whether the continuity of information security is captured within

> "Failing to plan is planning to fail."
>
> – *Alan Lakein*– American writer

the business continuity management process or within the disaster recovery management process.

Information security requirements should be determined when planning for business continuity and disaster recovery.

In the absence of formal business continuity and disaster recovery planning, information security management should assume that information security requirements remain the same in adverse situations, compared to normal operational conditions. Alternatively, an organization could perform a business impact analysis for information security aspects to determine the information security requirements applicable to adverse situations. (NL ISO/IEC, 2015)

12. Implementing Information Security Continuity

The organization should establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

An organization should ensure that:

a) an adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience and competence;
b) incident response personnel with the necessary responsibility, authority and competence to manage an incident and maintain information security are nominated;
c) documented plans, response and recovery procedures are developed and approved, detailing how the organization will manage a disruptive event and will maintain its information security to a predetermined level, based on management-approved information security continuity objectives.

Within the context of business continuity or disaster recovery, specific processes and procedures may have been defined. Information that is handled within these processes and procedures or within dedicated information systems to support them should be protected. Therefore an organization should involve information security specialists when establishing, implementing and maintaining business continuity or disaster recovery processes and procedures. (NL ISO/IEC, 2015)

13. Verify, Review and Evaluate Information Security Continuity

The organization should verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

Organizational, technical, procedural and process changes, whether in an operational or continuity context, can lead to changes in information security continuity requirements. In such cases, the continuity of processes, procedures and controls for information security should be reviewed against these changed requirements.

Organizations should verify their information security management continuity by:

a) exercising and testing the functionality of information security continuity processes, procedures and controls to ensure that they are consistent with the information security continuity objectives;
b) exercising and testing the knowledge and routine to operate information security continuity processes, procedures and controls to ensure that their performance is consistent with the information security continuity objectives;
c) reviewing the validity and effectiveness of information security continuity measures when information systems, information security processes, procedures and controls or business continuity management/disaster recovery management processes and solutions change.

The verification of information security continuity controls is different from general information security testing and verification and should be performed outside the testing of changes. If possible, it is preferable to integrate verification of information security continuity controls with the organization's business continuity or disaster recovery tests. (NL ISO/IEC, 2015)

14. Redundancies and Availability of Information Processing Facilities

The objective is to ensure availability of information processing facilities.

Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

Organizations should identify business requirements for the availability of information systems. Where the availability cannot be guaranteed using the existing systems architecture, redundant components or architectures should be considered.

Where applicable, redundant information systems should be tested to ensure the failover from one component to another component works as intended.

The implementation of redundancies can introduce risks to the integrity or confidentiality of information and information systems, which need to be considered when designing information systems. (NL ISO/IEC, 2015)

Glossary

BCP: Business Continuity Planning

CIA: Confidentiality Integrity Availability

CSO: Chief Security Officer

DMZ: Demilitarized Zone

DoS: Denial of Service

FTP: File Transfer Protocol

GPS: Global Positioning System

IT: Information Technology

LAN: Local Area Network

PC: Personal Computer

PIN: Personal Identification Number

ROI: Return On Investment

TCP/IP: Transmission Control Protocol/Internet Protocol

USB: Universal Serial Bus

VLAN: Virtual LAN

References

Abu Dhabi Systems and Information Centre. (2013). *Information Security Standards* (2nd ed.). Abu Dhabi: Abu Dhabi Government. Retrieved from https://www.abudhabi.ae

Albright, J. (2002). The Basics of an IT Security Policy - 103278. Retrieved July 30, 2014, from http://www.giac.org/paper/gsec/1863/basics-security-policy/103278

National Center for Education Statistics. (1998). Safeguarding Your Technology, Chapter 5- Protecting Your System: Physical Security. Retrieved November 12, 2014, from https://nces.ed.gov/pubs98/safetech/chapter5.asp

NL ISO/IEC. (2010). *Information technology - Security techniques - Code of practice for information security management (ISO/IEC 27002:2005)*. Lebanon: LIBNOR.

NL ISO/IEC. (2015). *Information technology - Security techniques - Code of practice for information security management (ISO/IEC 27002:2013)*. Lebanon: LIBNOR.

Stewart, J., Chapple, M., & Gibson, D. (2004). *CISSP Certified Information Systems Security Professional Study Guide* (6th ed.). Indianapolis, IN: Sybex, John wiley & Sons.