The Basics of Information Security

A Practical Handbook

This book is recommended as a study book for the Information Security Foundation based on ISO/IEC 27002 exams of EXIN.

EXIN is an independent, international examination institute for IT professionals. EXIN's mission is to improve the quality of the IT sector as well as that of IT professionals. In order to achieve these goals, EXIN develops exam requirements and IT exams.

EXIN provides four examinations in Information Security. These examinations are based on ISO/IEC 27002. You can take exams at Foundation, Advanced and Expert level. At Expert level you are tested not only on your knowledge of ISO/IEC 27002 but also of ISO/IEC 27001.

ISBN/EAN: 978-90-813341-1-2

Title: The Basics of Information Security - A Practical Handbook

Version: 18g

Date: March 1, 2009

Table of contents

1. Foreword

The word security has by nature a negative feel to it. Security is, after all, only applied when there is reason to: when there is a risk that things will not go as they should.

Security is therefore all to do with protection. Something has been done to reduce the chance of problems or to minimize their consequences. A spare tire, fireproof children's pajamas and insurance policies are all forms of security. A spare tire ensures that we are less troubled by a flat tire, the insurance policy covers financial consequences and fireproof pajamas reduce the risk of serious physical injury to a child.

Information has become a valuable commodity in our society. We can see this more clearly if we realize that not a single business process can be carried out without information. After all, the control of processes is always based on management information. Many companies do nothing else but process information. This is particularly the case for the financial sector and government. The business services sector as well does not do much more than collect information and then present it in another form.

Information even plays an important role in our spare time. Music, books and films in digital format (MP3, CD, DVD), the Internet and gaming all make use of digital information. The almost explosive growth of digital cameras, as well as mobile phones, has resulted in an inestimable number of photos that are stored as information on hard disks, portable players, CDs, DVDs and USB sticks.

It is therefore not surprising that in the last ten years the subject of information security has become of great interest to businesses, government and at home.

This book deals with the subject of information security in a manageable way. The chapters have been arranged so that the subjects are divided along clear lines. What's more, the technical measures, for example, have been treated in such a way that they are easy to understand for the non-IT specialist.

There is a connection between risk and security: if there were no risk there would be no need for setting up any security. And this is the same at home. Security costs time and money, and so if we can avoid it, we will.

The type and number of measures that are taken depend on the risk.

After the general introduction and an explanation of information and its value, the book examines threats and risks. Examining which risks are the greatest and which consequences are not acceptable is the subject of a risk analysis. The field of information security determines which measures have to be taken regarding these risks and threats. The analysis also determines the arguments for dealing with these risks.

Before discussing the measures, chapter 4 examines how to deal with information security in an organization. Subjects such as organization, management and quality requirements are looked at. Chapter 5 examines threats and the risk analysis. Chapter 6 then takes a closer look at information security incidents and weaknesses.

The subsequent three chapters examine measures. It is impossible to deal with all the available measures as new measures are being developed even as we write. The most widely used principles, however, will be examined. If you wish to find out more (technical) details about these measures we recommend contacting the relevant producers.

This book divides the measures into three groups:

- Physical measures, such as locks and fences, but also cabinets and reception desks;
- Technical measures, such as backups, software for codes and antivirus functions;

- Organizational measures such as the segregation of duties, confidentiality agreements and authorizations whereby it is arranged what a person is permitted to do in the information system.

The book is then concluded with a discussion on the applicable regulations and legislation. There are certain laws that impose statutory obligations to carry out security measures, for example personal data protection legislation which sets requirements for the protection of personal privacy.

Jacques Cazemier

2. About the authors

This book has been written by the same group of authors who wrote the Dutch book "The Netherlands goes digital, but securely", which was issued in 2002 as a joint publication of the Ministry of Economic Affairs and the Association of Information Security Specialists that is currently known as Platform for Information Security.

The authors are all members of the Dutch Platform for Information Security and aim to make the field of information security more accessible for information security specialists and departmental staff that are just starting out.

Hans Baars, CISSP, worked as information security officer and internal EDP Auditor at the police from 1999 to 2002. In 2002 he became consultant of integral security at the Dutch National Police Services Agency. In this position, he was involved in formulating the information security policy of the Dutch police force. Since 2006, he has been working as a security consultant. He advises government and commercial businesses on how to design their physical and information security in an affordable and workable manner.

Kees Hintzbergen is account manager at 3-Angle. Kees has more than 20 years' experience in IT and Information Provision and has worked in the field of information security since 1999. In 1998, he obtained his AMBI (Computerization and Mechanization of Information Provision Management) Masters in Exploitation and Management. He is certified in Business Informatics at the Hogeschool van Amsterdam and the Hogeschool Dirksen (System Engineer). He also attended the complete VAX-VMS training course at the former Digital. In his everyday life, Kees is a consultant, coach and 'mirror' whereby he employs the Common Sense Method. Thanks to his experience and his integrity, he is able to sell with his advice.

Jule Hintzbergen CISSP PSP, after working initially for 21 years for the Ministry of Defense, has worked since 1999 at Capgemini as a public security consultant. Jule has more than 20 years' experience in IT and spends much of his time dealing with information security. After obtaining an AMBI in Exploitation and Management in 1997 he worked in various capacities in the area of project management, information management, physical and information security and biometrics. He has for some time now worked with EXIN (Examination Institute for Information Science) on producing questions and as a reviewer. Since 2003 Jule has been a CISSP at ISC2 and since 2007 a PSP at ASIS International.

André Smulders (CISSP) is a senior information security consultant at TNO Information and Communication Technology. When André completed his Technology Management studies at the Technical University of Eindhoven he started in 1996 to work in the field of innovation and IT and since 2000 has specialized in information security. In his current role as consultant and project manager he has been involved in information security projects varying from a technological level to a strategic level.

This book has been reviewed by the following persons to whom we are most grateful:

Erno Duinhoven CISSP

Ben Elsinga CISSP

John van Huijgevoort

Joris Hulstijn

Fred van Noord

Marcel Oogjen

Rita Pilon

Jurgen van der Vlugt RE CISA

The Basics of Information Security - A Practical Handbook

Monika Vroege-Pokrzywa

This book was originally written in Dutch.

Translation:

Newton Translations, the Netherlands

The translation has been reviewed by:

Quinn R. Shamblin, Information Security Officer, University of Cincinnati, USA

Foreword by Jacques A. Cazemier.

Jacques A. Cazemier works as executive consultant in Information Security and Business Continuity Management (BCM) at Verdonck, Klooster & Associates (VKA). He was there at the very beginning when Information Security and Business Continuity Management were first implemented in the Netherlands in the mid-nineteen nineties.

In recent years he has been particularly active in the policy, organizational and planning aspects of information security for the government, businesses and financial institutions.

He has also been involved in investigating the status of information security, supervising investigations into computer break-ins and setting up Business Continuity Management.

He is senior lecturer for the MSIT (Master of Security in Information Technology) and the MISM (Master of Information Security Management) programs organized at the TiasNimbas Business School in collaboration with Eindhoven University of Technology in the Netherlands. He is also affiliated with TopTech of the Delft University of Technology and is guest lecturer at the Haagse Hogeschool and Saxion University in the Netherlands.

He is one of the authors of the ITIL® book Security Management.

Glossary

The glossary contains an explanation of concepts in relation to information security which appear in the text before they have been discussed in detail. The list is not exhaustive. It can be used as a tool in order to enhance the readers' understanding of the terminology applied in this book.

- **Algorithm:** a sequence of finite instructions, often used for data processing and calculation.
- **Availability of information:** the degree to which information is available for the user and for the information system that is in operation the moment the organization requires it.
- **Botnets:** a network of infected computers. See Storm Worm botnet.
- **Business assets:** everything of value that is owned by a company (examples: information, software, equipment, media, services, people and their knowledge but also reputation of the organization).
- **Clean energy:** refers to the prevention of peaks and troughs (dirty energy) in the power supply.
- **Compliance:** can be described as tractability, obligingness, pliability, tolerance and dutifulness. What it boils down to is that an organization must observe the organization's internal regulations as well as the laws of the country and requirements of local legislation and regulations.
- **Confidentiality:** the degree to which access to information is restricted to a defined group of persons authorized to have this access. This also includes measures to protect privacy.
- **Continuity of information systems:** the availability of information systems the moment that they are required.
- **Crimeware**: a class of malicious software designed to infiltrate or damage a computer system designed specifically to automate financial crime.
- **Disaster:** a large incident whereby the continuity of the company is threatened. Also the failure of the system upon which you depend so much for your daily work, through a technical problem, is a disaster.
- **E-commerce:** the buying and selling of products or services over electronic systems such as the Internet and other computer networks.
- **Encryption**: the process of transforming information (referred to as plaintext) using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.
- **Firewall**: an integrated collection of technical security measures designed to prevent unauthorized electronic access to a networked computer system.
- **Functional escalation (horizontal):** involving personnel with more specialist skills, time or access privileges (technical authority) to solve the incident.
- **Hacker:** in this book: a person committed to circumvention of computer security. This primarily concerns unauthorized remote computer break-ins via a communication networks such as the Internet.
- **Hierarchical escalation (vertical):** involving a higher level of organizational authority, when it appears that the current level of authority is insufficient to ensure that the incident will be resolved in time and/or satisfactorily.

- **IT infrastructure:** all information technology assets (hardware, software, data), components, systems, applications, and resources.
- **Incident:** any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in the quality of that service.
- **Information security incident:** a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
- **Integrity:** the degree to which the information is up to date and without errors. The characteristics of integrity are the correctness and the completeness of the information.
- **Logic bomb:** a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.
- **Logical access management:** it ensures that unauthorized persons or processes do not have access to automated systems, databases and programs. A user, for example, does not have the right to change the settings of the PC.
- **Malware:** software designed to infiltrate or damage a computer system without the owner's informed consent.
- **Non-disclosure agreement** (NDA): a contract through which the parties agree not to disclose information covered by the agreement. An NDA creates a confidential relationship between the parties to protect any type of confidential and proprietary information or a trade secret. As such, an NDA protects non-public business information.
- **Patch**: a small piece of software designed to fix problems with or update a computer program or its supporting data.
- **Phishing:** a form of internet fraud, attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.
- **Public Key Infrastructure** (**PKI**): a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates.
- **Reliability of information:** a quality requirement covering the confidentiality, integrity and availability of information (so-called “CIA” requirements).
- **Risk avoiding:** a risk strategy whereby measures are taken to neutralize the threat to such an extent that the threat no longer leads to an incident.
- **Risk bearing:** a risk strategy in which certain risks are accepted, for example because the costs of the security measures exceed the possible damage.
- **Risk neutral:** a risk strategy whereby measures are taken such that the threats either no longer manifest themselves or, if they do, the resulting damage is minimized.
- **Risk:** possible damage to or loss of information.
- **Rootkit:** a set of software tools that are often used by a third party (usually a hacker) after having gained access to a (computer) system. The rootkit hides itself deep in the operating system, possibly resulting in the operating system becoming unstable.
- **Segregation of duties:** used to determine as to whether a person carries out decision-making, executive or control tasks in order to avoid the chance of unauthorized or unintended changes or the misuse of the organization’s assets. It is determined whether the person needs access to information. Unnecessary access increases the risk of information being intentionally or unintentionally used, altered or destroyed. This is called the ‘need to know’ principle.

- **Spam:** a collective name for unwanted messages. The term is normally used for undesired e-mail, but undesired advertising messages on websites are also regarded as spam.
- **Spyware:** a computer program that collects information on the computer user and sends this information to another party. The purpose of this is to make money. Spyware does not purposely try to damage the PC and/or the installed software, but rather to violate privacy.
- **Stand-by arrangement:** a repressive measure, whereby fall-back means are put into service on an emergency basis in the event of a disaster. For example, using a different location (stand-by location) in order to continue to work.
- **Storm Worm botnet**: a remotely-controlled network of "zombie" computers (or "botnet") that has been linked by the Storm Worm, a Trojan horse spread through e-mail spam.
- **Threat:** anything (man made or act of nature) that has the potential to cause harm. The likelihood that a threat will use a vulnerability to cause harm creates a risk.

3. Introduction to basic information security

This book gives a general overview of information security. Information security is the discipline that focuses on the quality (reliability) of information provision and the continuity of operational management. Quality in this context is understood to mean the availability, confidentiality and integrity of the information. This book explains what these quality requirements entail, how they can be determined and what is necessary to ensure these in an organization. This field encompasses the work of the information security specialist. The subjects that play a role here are discussed in more detail in the relevant chapters. Each chapter will explain why the specific subject is relevant. This will be clarified using cases from everyday practice. These cases will be as generic as possible and not specific to any particular type of organization.

After reading the book you will have a general understanding of the subjects that encompass information security. You will also know why these subjects are relevant and will gain an understanding of the most common concepts of information security.

This book is intended for everyone in an organization who wishes to have a basic understanding of information security. This basic understanding is important to all personnel in a company or government as they all work with information. Line managers need to have this understanding as they are responsible for the security of information in their department. This basic knowledge is also important for all business people, including those self-employed without employees, as they are responsible for protecting their own information. A certain degree of knowledge is also necessary at home. And of course, this knowledge forms a good basis for those who may be considering a career as an information security specialist, whether as an IT professional or a process manager.

Every one of us in our daily lives is involved with information security, often in the form of measures. These measures are sometimes enforced upon us and sometimes we have implemented them ourselves. Consider, for example, the use of a password on the computer. We often experience measures as a nuisance as these often take up our time and we do not always know against what the measures are protecting us.

The trick to implementing information security is to balance a number of aspects:

- The quality requirements an organization may have for the information;
- The risks for these quality requirements;
- The measures that are necessary to minimize these risks;
- Ensuring the continuity of the organization in the event of a disaster.

The primary objective of this book is education. This is why each chapter ends with a case study. In order to help the understanding and coherence of each subject, these case studies include questions regarding the areas covered in the relevant chapters. You will also be given many examples from real-life cases and recent events that illustrate the vulnerability of information. It is not our intention to frighten you with these events, but rather to make you aware.

Due to its general character, this book is also suitable for awareness training or as a reference book in an awareness campaign.

In this book we tend to talk about large organizations, but the subjects covered are also applicable to the daily home environment as well as small organizations and companies that do not have any separate information security positions. In such situations the various information security functions would be carried out by a single person.

4. Information, business objectives and quality requirements

Introduction

As the name suggests, information security is all about ensuring the security of information. What security is exactly will be examined later. First we will have a look at information. Information is quite a broad concept and has many different definitions. These definitions are often related to a specific field or application. In this book we use the definition given in the Webster dictionary which describes information as '*the communication or reception of knowledge or intelligence*'.

For the concept of information security we use the definition of the Dutch Platform for Information Security. Information security involves the definition, implementation, maintenance, and evaluation of a coherent system of measures that ensure the availability, integrity and confidentiality of the (manual and computerized) information provision.

4.1 Forms

We can make a distinction between data and information. Some data can be processed by information technology, but becomes information once it has acquired a certain meaning. In our daily lives we come across information in countless various forms. Information can take the form of text, but also of the spoken word and video images. When it comes to information security we must take into account the diverse forms in which information can be manifested. It involves, after all, the security of the information itself and not the form it takes. The form information takes does, however, impose some restrictions to the measures that are necessary to protect that information.

4.2 Information systems

The transfer and processing of information takes places via an information system. It should be pointed out that an information system is not necessarily the same as an IT system (Information Technology system). Every system whose purpose it is to transfer information is an information system. Examples of information systems are files in filing cabinets, mobile telephones and printers. In the context of information security, an information system is the entire combination of means, procedures, rules and people that ensure the information supply for an operational process. These are increasingly IT systems, as a result of which we are becoming increasingly dependent on the proper functioning of these IT systems. As we have already said, an IT system consists of technological means that are related to one another in some way. These means include:

- The workstation, which consists of the PC with the operating system software and other software;
- Data transport via a network, cabled or otherwise (wireless);
- Central servers, consisting of the server with an operating system and software;
- Data storage, for example disk space, e-mail and databases;
- Telephones with their exchanges and aerials.

In the news

Users of smart phones with the Symbian OS S60 are being warned about the Beselo worm. This worm can be spread via mms and bluetooth.

The worm is disguised as the file sex.mp3, love.jpg or beauty.rm. As a result, users believe that it is a multimedia file and so install the worm. After installation the worm spreads itself further. It also copies itself onto the phone's memory card.

F-Secure (mobile and computer security provider) advises users to ignore the request to install. "There is no reason for a picture to request an installation. Any picture or audio file that does this, is therefore in another form than the one in which it presents itself," writes F-Secure.

4.3 Value of information

As mentioned earlier, information is knowledge that someone has acquired. Information that has no significance is called data. Whether something is information or data is determined primarily by the recipient. While some people may consider a particular set of data uninteresting, others may be able to extract valuable information from it. The value of information is therefore determined by the value that the recipient attaches to it.

4.4 Information as production factor

The standard production factors of a company or organization are capital, (manual) labor and raw materials. In information technology, it is common to also regard information as a production factor. Businesses cannot exist without information. A warehouse that loses its customer and stock information would usually not be able to operate without it. Some businesses, such as an accountant's office, even have information as their only product.

4.5 Availability, Integrity and Confidentiality

In protecting the value of information, we look at three factors; these are the quality requirements that information has to satisfy. Information must be reliable, that is to say it must have the following properties: confidentiality, integrity and availability, the so-called "CIA" requirements. Instead of the term confidentiality, some companies use exclusivity.

In every request to carry out a risk analysis or for security advice, the consultant will give advice on the basis of these three cornerstones.

The starting point is the influence that the CIA requirements have on the value of the information:

- The importance of the information for the operational processes;
- The indispensability of the information within operational processes;
- The recoverability of the information.

What we understand availability, integrity and confidentiality to mean is explained below.

4.5.1 Availability

Availability is the degree to which information is available for the user and for the information system that is in operation the moment the organization requires it.

The characteristics of availability are:

- Timeliness. The information systems are available when needed;
- Continuity. The staff can carry on working in the event of a failure;
- Robustness. There is sufficient capacity to allow all staff in the system to work.

Examples of availability measures:

- The management and storage of data is such that the chance of losing information is minimal. Data is, for example, stored on a network disk, not on the hard disk of the PC;
- Backup procedures are set up. The statutory requirements for how long data must be stored are taken into account. The location of the backup is separated physically from the business in order to ensure the availability in cases of emergency;
- Emergency procedures are set up to ensure that the activities can recommence as soon as possible after a large-scale disruption.

4.5.2 Integrity

Integrity is the degree to which the information is up to date and without errors. The characteristics of integrity are the correctness and the completeness of the information.

In the news

According to the security company Finjan, computer criminals are using Argentinean and Malaysian crimeware servers to sell the logins of hospitals and other healthcare providers. Security specialists regularly find all sorts of interesting information on hacked servers. On this occasion, it concerns data from hospitals and healthcare providers, business information from an airline company, and tax and social insurance numbers obtained through identity theft.

Using the stolen patient data, criminals are able to acquire medicines and treatments which they can then sell. For the victims, this can have consequences on their insurance coverage and personal medical records, which may result in damaging and incorrect treatments, says Finjan. On the crimeware server, the company found the Citrix logins of an American hospital and other medical institutions.

Examples of integrity measures:

- Changes in systems and data are authorized. For example, one member of staff enters in a new price for an article on the website, and another verifies the correctness of that price before it is published.
- Where possible, mechanisms are built in that force people to use the correct term. For example, a customer is always called a ‘customer’, the term ‘client’ cannot be entered into the database.
- Users’ actions are recorded (logged) so that it can be determined who made a change in the information.
- Vital system actions, for example, installing new software, cannot be carried out by just one person. By segregating duties, positions and authorities, at least two people will be necessary to carry out a change that has major consequences.
- The integrity of data can be ensured to a large degree through encryption techniques, which protects the information from unauthorized access or change. The policy and management principles for encryption can be defined in a separate policy document.

4.5.3 Confidentiality

Confidentiality is the degree to which access to information is restricted to a defined group of persons authorized to have this access. This also includes measures to protect privacy.

Examples of confidentiality measures:

- Access to information is granted on a need to know basis. It is not necessary, for example, for a financial employer to be able to see reports of discussions with the customer.
- Employees take measures to ensure that information does not find its way to those people who do not need it. They ensure, for example, that no confidential documents are lying on their desk while they are away (clear desk policy).
- Logical access management ensures that unauthorized persons or processes do not have access to automated systems, databases and programs. A user, for example, does not have the right to change the settings of the PC.
- A segregation of duties is created between the system development organization, the processing organization and the user’s organization. A system developer cannot, for example, make any changes to salaries.
- Strict segregations are created between the development environment, the test and acceptance environment and the production environment.
- In the processing and use of data, measures are taken to ensure the privacy of personnel and third parties. The Human Resources department (HR) has, for example, its own network drive that is not accessible to other departments.
- The use of computers by end users is surrounded with measures so that the confidentiality of the information is guaranteed. An example is a password that gives access to the computer and the network.

4.6 Information architecture

Information security is closely related to information architecture. Information architecture is the process that is focused on the set-up of the information provision within an organization. As briefly described above, certain requirements are set for the information provision. Information security can help to ensure that the requirements set are realized in the information architecture. Information architecture is primarily focused on realizing an organization's information need and the manner in which this can be organized. Information security can support this process by ensuring the integrity, availability and confidentiality of the information.

In the news

Boeing's new 787 Dreamliner may have a serious security problem. According to the American Federal Aviation Administration (FAA) it is theoretically possible for passengers of the plane to log on to the plane's control system.

It appears that there is a physical connection between the computer network that provides passengers with internet access and the plane's navigation, communication and control systems.

This physical connection is a huge security problem as it gives hackers potential access to the most important systems in the airplane. According to the FAA, the best solution is to completely remove this physical connection.

Boeing has stated that the company was already aware of this report of the FAA and that it has since been working on a solution. According to Boeing, however, the passengers' network and the airplane system do not completely connect, and it should already be impossible to compromise the control system. IT specialists have responded to this by saying that any type of software firewall is insufficient to protect such an important system.

4.7 Operational processes and information

In a business environment there is a close connection between operational processes and information. An operational process is the process that lies at the very heart of the business. In an operational process, people work on a product or service for a customer. An operational process has the following steps: input, process and output.

There are various types of operational processes:

- The primary process. For example, manufacturing a bicycle or managing money.
- Guiding processes. For example, planning the strategy of the company.
- Supporting processes. For example, purchasing and sales or HR.

Information has become an important production factor in carrying out operational processes. One of the methods for determining the value of information is to check the role of the information in the various operational processes. Each operational process sets specific requirements for the information provision. There are processes that are very dependent upon the availability of

information—for example, the company's website—whilst other processes are more reliant upon the absolute correctness of the information, such as the prices of the products.

4.8 Information analysis

Information analysis provides a clear picture of how an organization handles information—how the information 'flows' through the organization. For example, a guest registers with a hotel through the website. This information is passed on to the administration department, which then allocates a room. The reception knows that the guest will arrive today. The domestic services department knows that the room must be clean for the guest's arrival. In all these steps, it is important that the information is reliable. The results of an information analysis can be used to design an information system.

4.9 Information management

Information management formulates and directs the policy concerning the information provision of an organization. Within this system, an information manager can make use of the information architecture and an information analysis. Information management involves much more than the automated information processing carried out by an organization. In many cases, the external communication and communication with the media form part of the information management strategy.

4.10 Informatics

The term informatics relates to the science of the logic used in bringing structure to information and systems. It is important to understand that informatics can be used to develop programs.

4.11 Summary

In this chapter you have learned about the various forms of information and information systems. You have also been introduced to the trio: Availability, Confidentiality and Integrity. Finally, you have seen how information security is important for the operational processes, the information architecture and information management.

4.12 Case study

A car manufacturer has planned to build fifteen thousand cars of a particular model this year. The manufacturer has a second model in development. This second model is currently still on the drawing table and a number of mock-ups have been made to help to further develop the ideas.

This manufacturer has a large number of suppliers supporting the manufacture of its products. There is a great deal of collaboration in the development of the new model as well as in the supply of parts for the car once under construction.

On the basis of this case study, in which way do the Availability, Confidentiality and Integrity requirements play a role in the development and construction of a car? Incorporate the Availability, Confidentiality and Integrity requirements on the two information flows that have been mentioned. Also look at the operational processes and how the information architecture and the information management play a role.

5. Threats and risks

Introduction

These days houses are no longer built without secure doors and windows. However, it is up to you whether these windows and doors are closed and locked. This decision is made on the basis of habit or a consideration of the risks. In areas where there are many break-ins, the occupants would usually lock the doors.

The threat in this case is the theft of personal property. The risk that you may be a victim of a break-in can be determined by the frequency of break-ins in the area. The question is whether it is an objective risk. Are there really so many break-ins in the area? The risk estimation is subjective if you act on the basis of rumors only.

In the process of information security undesired effects (threats) are mapped out as well as possible. It can then be determined whether something must be done to avoid these effects and what that might be. The undesired effects to be avoided are not always clear for those who have to carry out the measures. Why do we have to change our password every three months? Other measures are less visible, such as the backups of the files on the server that are carried out at night. We only see the benefits of this when we lose a file.

We will now take a general look at how measures are established and what they are intended to achieve.

Before we start with our security measures, we need to know what we are protecting ourselves against. The methodology we employ to help us acquire some insight into this is called risk analysis. There are various forms of risk analyses. We will discuss a number of these in this chapter.

A risk analysis is used to outline the risks that an organization faces. A risk, possible damage to or loss of information is determined by a number of factors. These are the threat, or rather the chance that a threat will actually arise, and its consequences.

In practice

- A fire can break out at your company.
- An employee who does not work at the HR department gains access to HR information.
- Someone poses as an employee and tries to gain information.
- Your company is hit by a power failure.
- A hacker manages to gain access to the company network.

The information security uses lists of standard threats. The above threats are a small example of such a list.

When a threat manifests itself, such as when a hacker manages to get into the company network, we call that an incident. A power failure, such as the one in 2008 when a helicopter damaged a high-voltage cable, is such a large incident that the continuity of the company is threatened. We refer to this as a disaster.

When a threat materializes, a risk for the organization arises. Both the extent of the risk and management's assessment determine whether measures have to be taken in order to minimize the risk and what they may be.

In the news

The SANS Institute (System, Audit, Network, Security) has put together a list of the ten largest computer threats. The most striking threats are cyber espionage by governments, attacks on mobile phones and the spread of malware through consumer products such as USB sticks.

According to the SANS Institute the greatest computer threat of 2008 comes from websites that try to exploit vulnerabilities in browsers and their accompanying plug-ins (such as Flash and QuickTime). In second place, SANS expects a more sophisticated attack from botnets, following the Storm Worm which shook the world last year.

A striking third place on the list, is the cyber espionage perpetrated by large organizations and even governments. In 2007, China was frequently in the news due to its suspected spying practices. SANS is expecting to see more activities in this area from even more organizations.

Also the risk of attacks on mobile phones and VoIP systems is high on the list (fourth place). Telephones are becoming increasingly more sophisticated—often having a complete operating system—and, as a consequence, are becoming more vulnerable.

An old acquaintance is in fifth place: the users and workers themselves remain a weak link in the security surrounding (company) data. SANS advises companies to, for example, strictly restrict system access to what the user needs in order to be able to carry out his work effectively.

In sixth place is the risk of bots that inspect PCs for three to five months in order to collect data such as passwords, e-mail addresses, bank details, browsing history and the like.

In seventh place is the increasing maliciousness of spyware. According to SANS this type of software will become even better at identifying and knocking out anti-malware software, making it much more difficult to remove spyware from a PC.

In the lower regions of the list are the exploitation of vulnerabilities in web applications (eighth place), social engineering (employing the users of the systems to gain access to systems, for example through phishing) (ninth place), and the spread of malware through consumer products such as USB sticks, photo lists and GPS systems (tenth place).

The process from threats to risks and then to security measures is called risk management.

Risk management is a continuous process in which risks are identified, examined, and reduced to an acceptable level. This ongoing process applies to all aspects of the operational processes. In large organizations, the task of monitoring this process is carried out by an information security specialist, such as an Information Security Officer (ISO) or Chief Information Security Officer (CISO appointed especially for this role and who is responsible to the highest level of management).

This chapter will explain how a risk analysis works in practice.

5.1 Risk analysis

Risk analysis is a tool that is used in risk management. The purpose of carrying out a risk analysis is to clarify which threats are relevant to the operational processes and to identify the associated risks. The appropriate security level, along with the associated security measures, can then be determined.

A risk analysis is used to ensure that the security measures are deployed in a cost-effective and timely manner, and consequently provide an effective answer to the threats.

Security is a complex issue, even for experienced security specialists. It is not easy to find the right balance between security measures that are too stringent and those that are ineffective or inappropriate. A great deal of money is spent on unnecessary security measures due to not having a well thought out security concept as foundation. An aid that can help to arrive at a well thought out security concept is the risk analysis.

A risk analysis helps the company to correctly assess the risks and determine the correct and balanced security measures. Management can also find out the costs that are involved in taking the appropriate measures.

A risk analysis has four main objectives:

1. To identify assets and their value
2. To determine vulnerabilities and threats
3. To determine the risk that threats will become a reality and disrupt the operational process
4. To determine a balance between the costs of an incident and the costs of a security measure

Part of the risk analysis is a cost/benefit assessment. The annual costs associated with the security measures are compared with the potential losses that would occur if the threats were to become reality.

The organization must take care to avoid a situation where a server, including the data, is worth 100,000 Euros and that the security measures taken cost 150,000 Euros. That said, such situations do actually sometimes happen. Statutory requirements for protecting data can sometimes force companies to take measures that actually cost more than the value of the assets being protected.

Mind you, it is not easy to determine the value of data. Consider, for example, the damage to the organization’s reputation caused by a security incident. It is difficult to calculate the damage caused.

5.2 Types of risk analysis

There are two main groups of risk analyses: the quantitative and the qualitative risk analysis.

5.2.1 Quantitative risk analysis

The quantitative risk analysis aims to calculate, basing on the risk impact, the level of the financial loss and the probability that a threat may become an incident. The value of each element in all operational processes is determined. These values can be comprised of the costs of the security measures, as well as the value of property itself including such items as buildings, hardware, software, information and business impact. The time spans before a threat appears, the effectiveness of security measures and the risk that a vulnerability will be exploited are also elements to be considered.

In this way, a clear picture is provided of the total financial risk and appropriate measures may be determined. An important part of this is determining which residual risks are acceptable to the

managers responsible. The costs of the measures must not exceed the value of the protected object and the risk.

A purely quantitative risk analysis is practically impossible. A quantitative risk analysis tries to assign values to all aspects, but that is not always possible. A defective server can be assigned a value: the purchase value and the depreciation of the server, the value of the software that has to be installed, and the wage costs associated with any repairs can all be determined. But just try giving a value to the damage caused to a company. How much value loss does a company suffer when certain data is lost? This is sometimes possible to determine, but not always.

This can make it difficult to determine the correct measures for preventing damage.

In practice

- You own an insurance office and the details of policy holders become public through a fault of an employee. How many clients will you lose as a result?
- The personal details of witnesses in a criminal case are leaked. How many people would still be willing to testify in the trial?
- An employee has lost a USB stick and the press goes to town on this. How reliable is your organization now in the eyes of the public?

5.2.2 Qualitative risk analysis

A qualitative risk analysis is based on scenarios and situations. In this approach, the chances that a threat becomes reality are examined on the basis of gut feelings. The analysis then examines the operational process to which the threat relates and the security measures that have already been taken. This all leads to a subjective view of the possible threats. Measures are subsequently taken to minimize the risk. The best result is achieved by carrying out the analysis in a group session, as this leads to a discussion which avoids the view of a single person or department dominating the analysis.

Quantitative and qualitative risk analyses each have their own advantages and disadvantages. Management, in consultation with specialists, determines which method should be applied in which situation.

5.3 Measures that reduce the risk

The risk analysis produces a list of threats and their relative importance. The next step is to analyze each serious threat and to find one or more measures that can reduce that threat. The measures may be aimed at reducing the chance of the event occurring, at minimizing the consequences, or a combination of the two.

5.3.1 Types of security measures

How do we construct the security solution? This can be done in various ways and depends on the objectives. Security measures should always be linked to the results of a risk analysis and based on the reliability aspects and characteristics of information.

What do we wish to achieve?

1. Reductive measures are aimed at reducing the threats;
2. Preventive measures are aimed at preventing incidents;
3. Detective measures are aimed at detecting incidents;
4. Repressive measures are aimed at stopping the consequences of an incident;

5. Corrective measures are aimed at recovering from the damage caused by an incident.

- It is also possible to buy insurance against certain incidents because, for example, implementing the measures may be too expensive.

Depending on the level of the risks we can also choose to accept certain risks.

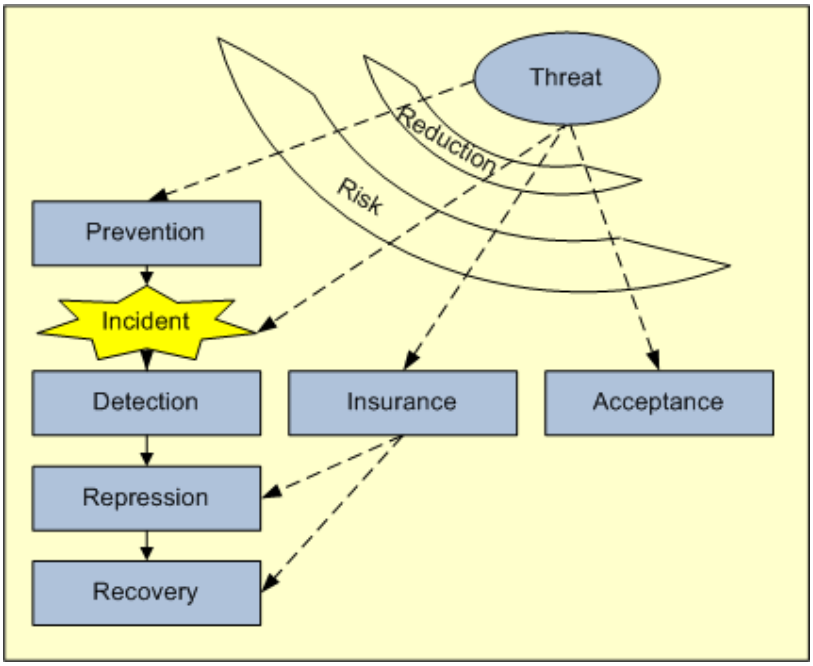


Figure 1: Security measures

5.3.2 Prevention

Prevention makes the threat impossible. Examples include breaking the connection with the internet and bricking up the door. These are not very practical to say the least, but there are other preventive measures that are more practical. Placing sensitive information in a safe is an example of a preventive measure.

5.3.3 Detection

If the direct consequences of an incident are not too great, or if there is time to minimize any consequential damage, then detection can be a good option. Ensure that each incident can be detected as quickly as possible and that everyone is informed that this is being done. An example of this is video surveillance with stickers on the windows informing people they are being monitored. Simply informing people that internet use is being monitored will dissuade many employees from improper internet browsing activities. Traceability plays a growing role in society and seems to be leading to a shift in the burden of proof. In the event of suspicions, the organization has to show that there were *no* irregularities.

5.3.4 Repression

Determining that something has happened is not enough. When something actually does go wrong—an incident occurs—the thing to do is to minimize the consequences. There is, for example, no point in having fire extinguishers if someone then does not take the initiative to use them to put out a small fire. Repressive measures, such as putting out a small fire, are aimed at minimizing any damage that may be caused. Making a backup is also an example of a repressive measure. After all, making a

periodic backup whilst working on a document ensures that the work is not totally lost if an incident were to occur. The backup can restore the document so only a part of the work is lost.

A stand-by arrangement is also an example of a repressive measure, whereby fall-back means are put into service on an emergency basis in the event of a disaster. For example, using a different location in order to continue to work.

5.3.5 Correction (Recovery)

If an incident has occurred, there is always something that must be recovered. The extent of the damage, very small or very large, depends on the repressive measures that were taken. For example, if a colleague were to make a new database that overwrites the previous database, then the extent of the damage depends on the backup. The older the backup, the greater the damage.

5.3.6 Insurance

For events that cannot be entirely prevented and for which the consequences are not acceptable, we look for methods that can alleviate the consequence. This is called mitigation. Fire insurance protects us against the financial consequences of a fire. Placing a copy of all important information to a location outside the organization every day ensures that, after the fire, we at least still have the irreplaceable information. Both measures are not cheap, but are usually regarded as justified.

5.3.7 Acceptance

When all measures are known, it may well be decided not to carry out certain security measures as the costs are not in proportion to the return, or because there are no suitable measures possible that can stand up to the risks.

5.4 Types of threats

Threats can be divided into human threats and non-human threats. When working to determine threats, information security professionals will often refer to standard lists of threats. It is necessary to determine which threats are relevant and which are not. Security, after all, requires organizations to spend money and it is not sensible to invest in security against threats that will not occur.

In practice

If your company is located in an area that has never experienced an earthquake, there is no point in taking earthquakes into account; so no measures need to be taken against these.

We will now look more closely at the types of threats.

5.4.1 Human threats

Intentional human threat. People can intentionally cause damage to information systems for various reasons. We usually think of outsiders such as a hacker who has something against a company and wishes to break into it and cause it damage.

However, what about a company employee who destroys company data after being dismissed, or who, not getting the promotion he or she wanted, takes revenge by destroying data or selling it to the competition.

We are again talking in terms of digital information, but this could of course also involve the physical destruction of information or even the equipment. We probably all know the advertisement of the frustrated office worker throwing his computer out of the window.

Social engineering makes use of people—tricking them into voluntarily providing sensitive information such as company and trade secrets. The social engineer takes advantage of weaknesses in people in order to realize his or her objectives. We are often not aware of this and do not know that a social engineer is at work. If you come across a stranger in the corridor, ask him whether you can help him. If the helpdesk phones you asking where a particular file is, ask or check whether you are actually talking to the helpdesk. Do you ever talk about your work on the train, and are you sure that you do not mention anything confidential? A social engineer works according to a certain pattern. We could write a whole book about social engineering, but will leave it at this for now.

Unintentional threat. People can also cause damage unintentionally. For example, accidentally pressing the delete button and carelessly confirming this with OK. You could also insert a USB stick that has a virus into a machine and spread the virus throughout the network. In panic, you may use a powder extinguisher to put out a small fire and consequently destroy a server. These are typical human responses whereby good security measures are inappropriately applied or subverted.

In the news

Intentional or unintentional?

How the White House managed to lose ten million e-mails will always be a mystery now that an American court has ruled that the Executive Office of the President does not have to give any information on this. The Civil Rights group 'Citizens for Responsibility and Ethics in Washington' (CREW) wanted to know through the Freedom of Information Act (FOIA) what was contained in these messages and why they disappeared.

According to the supreme court, the Executive Office does not fall under this law, due to an amendment that the Bush government made in 2006 and 2007. CREW believes that the White House has possibly tried to sweep lobby scandals, suspected political influence on the General Services Administration responsible for government spending, and other embarrassing matters under the carpet by disposing of these messages.

"The Bush government uses the legal system to prevent the American people from discovering the truth about the millions of lost e-mails at the White House," said disappointed CREW director Melanie Sloan.

5.4.2 Non-human threats

There are also non-human threats, external influences such as lightning strikes, fire, floods and storms. Much of the damage caused will depend on the location of the equipment in the premises. Is the server room located directly under a flat roof that is susceptible to leaking? Is it situated underground in an area where there is high ground water? Does the server room have windows or is it located in a bunker-style room? All such concerns have an influence on the risks that the organization will face.

We can subdivide human and non-human threats into disruptions in the basic infrastructure such as computer equipment, software or databases and disruptions in the physical environment such as buildings, paper dossiers, electrical installations, water supplies, heating, ventilation and cooling.

In the news

A corrupted file had almost poured cold water on a firework display in Seattle. The team in charge of the show discovered the problem just one minute before twelve o'clock, and were able to detonate the fireworks manually at the last moment.

As a result, not only did the show last longer (11.5 minutes instead of 8.5), but the rockets were also released out of synchronization with the accompanying music. Spectators were nonetheless satisfied with the firework display, according to a local newspaper.

According to a company spokesperson, this was the first time in fourteen years that such a problem had occurred.

5.5 Types of damage

Damage resulting in the manifestation of the above threats can be classified as follows:

- Direct damage;
- Indirect damage;
- Annual Loss Expectancy (ALE);
- Single Loss Expectancy (SLE).

An example of direct damage is theft. Theft has direct consequences on the business.

Indirect damage is consequential loss that can occur. For example damage caused by the water from fire extinguishers or being unable to meet a contract due to the IT infrastructure being destroyed by fire.

In the news

An employee of an American company destroyed 2.5 million dollars worth of company data because she thought her boss wanted to fire her. The woman suspected the dismissal when she read a job advertisement that referred to a job so similar to her own that she thought it was her job being advertised. Angrily, the woman decided to log on to the company server and delete all the drawings and designs from the last seven years.

Although an IT consultant managed to retrieve the data, the woman is being charged with damaging the computers. What's more, the data that the employee wanted to delete is worth approximately 2.5 million dollars. Ironically, the advertisement that the woman had read was not even placed by the company for whom she worked. She can nonetheless probably forget about her job now.

A Single Loss Expectancy is the damage caused by a one-off incident.

The Annual Loss Expectancy is the amount of damage—expressed in monetary terms—that can result from an incident in one year. For example, assume that an average of 10 laptops are stolen from a company each year. The annual loss expectancy is therefore the value of 10 laptops (including the data and software), not just one laptop. A measure proposed to counter the theft of laptops may therefore cost more than the value of one laptop. However, if an incident were statistically to occur once every five years, then the annual loss expectancy is one fifth of the single loss expectancy.

Indirect damage is different. One example is the damage to a company's reputation.

Other Examples

- A company loses confidential personal data of its clients. It appears in great detail in the press and gives the organization a negative image. No advertising campaign can make amends for this.
- All clients of a big bank are not able to execute on-line transactions because the bank's website is overtaken by criminals.
- A company delivers standard software to its clients. The software turns out to be containing a virus.

5.6 Types of risk strategies

We can deal with risks in different ways. The most common strategies are:

- Risk bearing;
- Risk neutral;
- Risk avoiding.

By risk bearing, we mean that certain risks are accepted. This could be because the costs of the security measures exceed the possible damage. But it could also be that the management decides to

do nothing even if the costs are not higher than the possible damage. The measures that a risk bearing organization takes in the area of information security are usually of a repressive nature.

Risk neutral means that security measures are taken such that the threats either no longer manifest themselves or, if they do, the resulting damage is minimized. The majority of measures taken in the area of information security by a risk neutral organization are a combination of preventive, detective and repressive measures.

By risk avoiding, we mean that measures are taken such that the threat is neutralized to such an extent that the threat no longer leads to an incident. Consider, for example, the addition of new software which makes the errors in the old software no longer a threat. Described more simply, we could say that an iron bucket can rust; replace it with a plastic bucket and the threat of rust will be removed. Many of the measures within this strategy have a preventive character.

Regardless of the strategy an organization chooses, management has to make a conscious decision and bear the consequences.

5.7 Guidelines for implementing security measures

Implementing security measures thoroughly throughout an organization involves a great deal of work. At many companies, the IT system has developed over the course of the years from a single PC on which the administration was done to a large-scale network with many thousands of PCs and dozens if not hundreds of servers.

There are guidelines that help in choosing measures. A company can therefore present a more positive public image by making it clear that it meets these guidelines.

ISO/IEC 20000 is the worldwide standard for IT service management. While the ISO/IEC 27001:2005 standard deals with the set-up of the information security process. Both standards help in setting up the operational processes in an effective and secure manner.

The ISO/IEC 27002:2005 standard, which is also known as the ‘Code for Information Security’, contains guidelines for measures in the area of information security. The guidelines in the ISO/IEC 27002:2005 standard deal with the organizational, procedural, physical and logical aspects of information security.

In practice

Governments across the world have imposed legislation and regulations in order to protect certain information. This may be information regarding private individuals, as well as businesses and the government itself.

Dutch companies listed on the stock exchange, for example, have to abide by the Code Tabaksblat. For companies listed on the Dow Jones Stock Exchange in New York, the Sarbanes-Oxley Act (SOX) applies, both for American and foreign companies.

These are a few examples of legislation and regulations that compel companies to effectively organize their information security. Meeting the ISO/IEC standards in this area is one way of achieving this.

5.8 Summary

In this chapter, you have learned many new terms. We also examined the various types of threats and how to deal with them.

A risk analysis gives a clear picture of the risks an organization faces. What sorts of threats are there and what are the various types of damage?

What risk strategies do we have available?

Do we have to implement a measure for every risk or can we accept certain risks?

5.9 Case study

The fictitious Dutch municipality of Betuwegaard contains much of the Gelders river area. This municipality was created through merging seven previously independent municipalities. The old town halls now serve as branch offices for the local population. In the centre of the area, a new town hall is being built which will house the central administration and maintenance departments. The computing centre will also be located here, where seven computer systems will be combined to form a single central computer system.

The location is attractively situated alongside a dyke and water recreation area (a former sandpit). The civil servants look out over the river Waal, and during their afternoon breaks they can enjoy the water recreation possibilities there. A ferry provides a good connection to the other side of the river Waal, and a good road network ensures that there is easy access to the new town hall from the surrounding area. The main roads can be reached from a bridge over the river Rhine, only one-and-a-half kilometers away.

You are given the task of carrying out a risk analysis of the Betuwegaard council's new development plans.

- What sort of risk analysis will you carry out?
- What are the main risks that you identify?
- What aspects in particular does the Betuwegaard council have to take into account when they decide to proceed with the new development?

Control questions:

1. What is the purpose of a risk analysis?
2. What is the difference between a threat and a risk?
3. What types of measures are there?
4. What types of risk strategies are there?
5. What is the difference between a risk analysis and risk management?
6. What types of risk analysis methods are there?
7. What types of damage are there?

6. Business assets and information security incidents

Introduction

This chapter will explain business assets management and classification and their role in the information security process.

The information security process is not a one-time event; it is a continuous process. Every organization undergoes constant change, and so the threats, risks and measures also constantly change. Information security must be embedded within the organization and requires constant attention.

It is important that information security is supported by the highest management level within a company, and that this is clearly visible to all staff. Other processes form part of the information security process, such as incident management. What's more, the various tasks involved in the information security can, depending on the size of the organization, be carried out by different people of varying degrees of specialization.

6.1 What are business assets

Business assets are necessary for an organization. They cost money or have a certain value. Business assets include:

- Information in the form of documents, databases, contracts, system documentation, procedures, manuals, system logs, plans and handbooks;
- Computer programs, such as system programs, user programs and development programs;
- Equipment such as servers, PCs, network components and cables;
- Media;
- Services;
- People and their knowledge;
- Non-tangible assets such as the image and reputation of the organization.

Business assets must be classified in order to be able to set security levels for them. This is the responsibility of the owner. Each asset must have an owner and should be registered.

A good and complete registration of business assets is necessary for risk analysis (see: Threats and Risks). In addition, registration is sometimes necessary for insurance, financial accounting and statutory requirements (for example, the registration of personal data in accordance with legislation for personal data protection). It is best to audit the record of business assets twice per year, and to produce a report of this for management.

The information that is recorded about the business asset is:

- The type of business asset;
- Owner;
- Location;
- Format;
- Classification;
- Value to the business.

This information may be necessary, for example, after the recovery following an incident or disaster.

The owner is the person responsible for a business process, sub-process or business activity and takes care of all the aspects of the business asset including the security, management, production and development.

6.2 Managing business assets

One way of controlling or managing risks is to exert control on changes that pose some sort of risk. This control can be carried out in various ways. There are various models and methods available that help in exerting this control, for example in COBIT™ and ITIL®. Each of these models or methods has a number of basic elements that help in the control process. The basic elements are:

- Agreements on how to deal with the business assets;
- Agreements (processes) on how changes come about;
- Agreements on who may initiate and execute the changes, and how these changes will be tested.

A pitfall that arises when establishing these, often bureaucratically interpreted, agreements is that they can be elevated to an aim rather than focusing on their significance.

COBIT™ stands for Control Objectives for Information and related Technology and is a framework for setting up and assessing an IT environment in a structured way.

ITIL® stands for Information Technology Infrastructure Library and was developed as a frame of reference for setting up management processes within an IT organization.

6.2.1 Agreements on how to deal with business assets

The purpose of documenting how to deal with business assets is to avoid faults that may arise through incorrect use. Incorrect use can also lead to unnecessary damage. Consider, for example, a simple rule such as not putting paper that contains metal (paper clips, staples) into a paper shredder. The more complex the asset, the more useful it is to set down clear instructions and directions.

6.2.2 The use of the business assets

The use of business assets is subject to certain rules. These rules may be provided in a manual and may, for example, include instructions on how to use mobile equipment when outside the organization. Implementing such rules falls within the scope of organizational measures. See 9.4.10 Mobile equipment.

6.3 Classification

First of all, an explanation of a number of terms:

- **Classification** is to define different levels of sensitivity into which information may be structured;
- **Grading** is the act of assigning the appropriate classification—such as secret, confidential or public—to specific information. The term grading is used often within the government;
- **Designation** is a special form of categorizing of information, for example, according to a particular subject matter or organization or a group of authorized persons.
- The **owner** is the person who is in charge of a business asset. A folder on the network can, for example, have an owner. If someone wishes to have access to that folder, the owner would have to give permission. With laptops, the user is usually registered as the owner.

The owner of a business asset assigns an appropriate grading in accordance with an agreed list of classifications. The classification indicates the form of security that is necessary. This is determined in

part by the sensitivity, value, statutory requirements and importance to the organization. The classification is in accordance with the manner in which the business asset is used in the business. The owner of the business asset must ensure it is reclassified if necessary. If business assets within an organization have been classified, only the owner is able to lower this classification (the grading) or give permission to do so. Information, for example, may be classified as confidential up to the moment of publication, but once the information has been made public, the classification is reduced.

If an asset has a grading, it is given a mark or label. This can be placed physically and visibly on the business asset, such as on the computer monitor and on the transmission cables, or inside it, such as is the case with digital documents, databases, records, and messages. A measure for documents could be that the grading must be visible on a certain place on the document. All documents containing classified information must have a copy or version number and numbered pages. It must also be clear of how many pages the entire document consists. This is a fairly stringent measure, all the more so as it has to be possible to check the measures.

Practically all national governments use a system of hierarchical secrecy which assigns a level of sensitivity to data. From highest to lowest this is usually: Top Secret, Secret, Confidential and Restricted.

A designation can be added to this grading. This designation can indicate a specific group of authorized persons.

An example of this is: Police Highly Confidential, Cryptography.

A document with this grading and designation is only intended to be handled by personnel who are authorized to use encryption methods. Within government, people are screened up to the level the classification indicates. Other guidelines are also followed, such as access to information on a need to know basis and, of course, the clear desk policy.

The owner determines who has access to the particularly designated business assets. The grading of a business asset also determines how it can be stored physically. For this, business premises are sometimes divided into compartments, with different security requirements for each compartment and increasing level of security, see: Protection rings.

The use of a grading is very difficult to implement in an organization, as people have to think carefully if they are to apply grading properly. Another possibility is not to assign a grade to non-classified information. This information is public.

6.4 Managing information security incidents

Company staff play an important role in detecting weaknesses in security and noticing security incidents. They are, after all, the first to see the incident: someone has left a confidential document in the printer; a file with personal information has disappeared; there is an unusual odor in the room where the paper shredder is kept; a door that should be locked has been left open; a colleague is behaving erratically; the PC monitor is showing strange messages.

Staff members must be able to report incidents and the reports need to be acted upon. Usually staff members report such incidents to the helpdesk. The helpdesk employee identifies that this is indeed an information security incident and then carries out the relevant procedure for resolving the incident and reporting it further. If the helpdesk employee is not able to deal with the incident personally (due to insufficient technical knowledge), the incident can be reported to someone with more expertise who may be able to resolve the problem. This is called a functional (horizontal) escalation. An incident can also be reported to someone who has more authority and who can make a decision. This is called hierarchical escalation. An example of hierarchical (vertical) escalation is notifying one's manager of the suspicious behavior of a colleague.

The purpose of this incident management process is to gain insight into incidents and to learn lessons from them for the future. Such notifications can also initiate another information security process, such as the recovery of a file, a security investigation, or even moving to a stand-by location.

6.4.1 Reporting information security incidents

There are various types of incidents and they occur to various degrees. The ISO/IEC 20000 standard describes how incidents can be managed in the incident management process. But not every incident is a security incident.

In practice

The IT service desk of a large organization is approached with the question: "*Can you tell me how in Word to get the bold letter function back in the toolbar at the top of my screen*". This question is recorded as an incident in the service desk system, though we cannot call it a security incident, unless there is a 'bold letter button removal virus' of which no one has as yet heard.

The purpose of the incident management process is to ensure that incidents and weaknesses that are related to information systems are known so that appropriate measures can be taken in time.

Staff, temporary personnel and external users should all be made aware of the procedures for reporting the various types of incidents and weaknesses that can have an influence on the Reliability of the information and the security of the business assets.

It should be required of staff and users to report all incidents and weaknesses as quickly as possible to the service desk or a contact person. It is, of course, in everyone's interest that the organization responds quickly.

Two matters are of great importance and have to be made clear by the management:

1. Reporting security incidents is primarily a way of learning from them so as to avoid similar incidents from occurring again;
2. Reporting an incident is not intended as a way of punishing the perpetrator of that incident.

However, this is not to say that this may not happen; if an employee were to intentionally sabotage an information system, leak information or cause damage, he or she would have to be reported to the police.

It is important that people not be afraid of reporting an incident out of fear for the management's response or not wanting to be seen as a telltale.

The process must also ensure that the person who reports an information security incident is informed of the results after it has been dealt with.

Incident reports are also useful when carrying out a (modified) risk analysis. It could be that the measures taken so far are not sufficient to prevent certain incidents.

A standard form on the intranet for reporting such incidents can help to reduce the fear and resistance to reporting. The form can be used not only for giving instructions on the immediate response to the incident that may be necessary but also for acquiring various details relating to the incident.

An incident report form should at a minimum allow the following information to be entered:

- Date and time
- Name of the person reporting
- Location (where is the incident?)

- What is the problem? (description of the incident: Virus incident, theft, break-in, data loss, etc.)
- What is the effect of the incident?
- How was it discovered?

And, if possible, the following areas:

- Type of system (desktop, printer, server, mail server, etc.)
- System number / system name (if present)
- Who else was informed?

Many other questions are also possible, depending on the type of report. It is important that sufficient information be collected so that the incident can be remedied correctly.

In practice

- No maintenance is carried out on the equipment;
- The emergency power supply has not been tested;
- A colleague loses a laptop;
- A colleague does not adhere to the clear desk policy;
- A colleague brings along an unauthorized visitor;
- New software is rolled out before being thoroughly tested;
- A virus has managed to get into the information system;
- Due to incomplete company data, the profit results are unreliable;
- The access rights of an employee are not modified after a change of job;
- Colleagues write their password on note paper that is lying on the PC.

Instructions on what to do in the event of an incident are usually formalized in published procedures. A procedure, after all, describes who does what. Such a procedure should include:

- The analysis of the incident; establishing the cause;
- What steps have to be taken to minimize the consequences of the incident;
- What steps have to be taken in order to determine if corrective measures are necessary in order to prevent the incident occurring again, and, if so which ones;
- Which parties are to be informed in the event of an incident. This could be those who are affected or those who help to resolve the incident;
- What is reported about the incident and to whom.

6.4.2 Reporting weaknesses in the security

When staff, temporary personnel and external users of information systems and services notice that there are (suspected) weaknesses in the system or services, it is important that they report those weaknesses as soon as possible. Only then can incidents be avoided.

When an information security incident is discovered, it is often not immediately clear whether the incident will lead to legal action. There is also the danger of critical evidence being destroyed either intentionally or unintentionally before the seriousness of the situation is realized. It is therefore important to first report the incident and then ask for advice on the action to take. It is possible that a lawyer or the police need to be involved at an early stage and that evidence will need to be collected.

In practice
If someone suspects that child pornography is being stored on a colleague's computer, the reporting of the incident has to be done carefully to ensure that no evidence is removed.

6.4.3 Registration of disruptions

In order to be able to analyze a disruption, it is important that the relevant information is collected. This information is often stored in log files. This is the modern version of the traditional logbooks that can still be used today. Imagine there is a power failure and there is no other way of recording the events and actions carried out other than on paper.

In large organizations, disruptions are reported to the service desk (helpdesk). If they are able to, they will resolve the disruption straightaway. If this is not possible, they will pass the relevant information on to a department that can resolve the disruption.

6.4.4 Incident cycle

The incident cycle has the following stages: threat, incident, damage and recovery.

Security measures are aimed at a certain moment in the incident cycle. The measures are intended to prevent incidents (preventive) or reduce the threats (reductive), detect incidents (detective), respond to incidents, stop threats (repressive) and to correct damage (corrective).

The measures are taken in order to ensure the availability, integrity and confidentiality of company information.

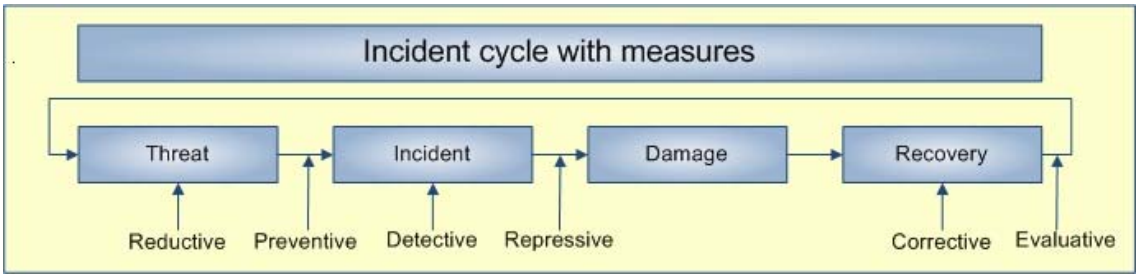


Figure 2: Incident cycle with measures

6.5 Roles

Depending on the size of the organization there can be various roles or positions for the various responsibilities in information security. These roles may vary in the title they are given, but they more or less come down to the following:

The Chief Information Security Officer (CISO) is at the highest management level of the organization and develops the general strategy for the entire business.
The Information Security Officer (ISO) develops the policy of a business unit based on the company policy and ensures that it is observed.
The Information Security Manager (ISM) develops the information security policy within the IT organization and ensures that this is observed.

In addition to these roles that are specifically geared to information security, an organization may have an Information Security Policy Officer or a Data Protection Officer.

6.6 Summary

In this chapter you were introduced to incident management. How does an organization deal with security incidents?

It is very important to report incidents; not only in order to be able to solve the incident and to consequently keep the threats and risks for an organization under control, but also in order to learn from them. After all, without knowledge of security incidents, we would not be able to avoid them in the future.

6.7 Case study

At a large government organization with branches located throughout the country, security incidents are a regular occurrence. Not so long ago, for example, an employee left his laptop on the roof of his car. The laptop was found, and the information it contained was not intended for everyone to see. USB sticks are also frequently being lost. Management believes much more is going on, but is not sure what exactly. The auditing department was unpleasantly surprised when it discovered that there was no security system in place. The director in charge justified this by saying that the personnel knew what they were and were not permitted to do! Under pressure from the auditing department, management appointed a number of people to be in charge of information security.

After a tense round of applications, you have the honor of becoming the first Information Security Officer (ISO) within this government department. Your primary task is to ensure that:

1. Information security is implemented according to current government legislation and regulations;

2. Staff are aware of the benefits and necessity of information security;

3. By the next ministerial audit, in two years' time, the information security is well organized and that incidents are a thing of the past.

What actions will you undertake and how will you carry them out?

7. Physical measures

Introduction

The previous chapters examined the organization of the information security and discussed risk analysis. A risk analysis results in a set of security measures that fit with the risk profile determined for the organization.

Some of the measures that result relate to the physical security of the organization. It all depends on the type of organization. For an organization that has a public function, access to the buildings and the site will be fairly unrestricted. An example of this is a public library. On the other hand, there may be organizations that make products only under very strict security. One example is an organization in the pharmaceutical industry that is subject to very stringent requirements in the area of hygiene and confidentiality regarding the formulae used.

This chapter will take a closer look at physical measures.

Physical measures are often implemented in combination with technical and organizational measures.

7.1 Physical security

Physical security is part of information security because all business assets must be physically protected as well. Physical security is older than information security; just think of the protection a castle provides those inside. Protecting information became important later. Traditionally, physical security is provided by the general and technical services managers who use their own particular methods and techniques to set up the physical security. In many organizations, the coordination between those in charge of physical security and information security is of great importance. We will also examine the various areas of responsibilities that those in charge of information security have to take into account.

The world of physical security employs a combination of organizational, structural and electronic measures. Physical measures need to be planned and coordinated in a coherent way. For example, attaching security cameras will only really be effective if structural measures have been taken and if careful thought has been given to their purpose and placement. What's more, the organization must follow up on anything detected or seen; otherwise installing a camera is totally pointless.

What is often forgotten is that physical measures also apply to temporary (emergency) locations.

7.1.1 Equipment

Physical security includes the protection of equipment through climate control (air conditioning, air humidity), the use of special fire extinguishers and the provision of 'clean' energy. Clean energy refers to the prevention of peaks and troughs (dirty energy) in the power supply and the fact that the power is filtered.

7.1.2 Cabling

Cables must be laid in such a way that no interference can occur. Interference is when the network cables pick up the noise and static from the power cables that run parallel with them. These effects are often not visible or audible. An example of this effect can be heard when mobile phones cause disturbance in speakers or radios. Cable ducts also have to be protected. Server rooms often use separate power supplies. It is not unusual for a server to have two power supplies, each connected to their own group.

7.1.3 Storage media

It must be clear to the employees of an organization how they should deal with storage media. Specific measures may apply to certain equipment; consider, for example, the deletion of confidential information on the storage media when a person leaves the organization. Storage media include more than just the obvious forms such as USB sticks and hard disks. Many printers can store information on their own hard disk. Documents can be temporarily stored on printers and can be partially retrieved.

It is also possible to store a great deal of information on mobile equipment, such as telephones, USB sticks, memory cards, organizers, blackberries, and laptops. It is important that if an employee leaves the company, that they return all their equipment, and that the information contained on them is deleted. There must also be procedures for when such equipment is lost or stolen.

7.2 Protection rings

All business assets have a certain value, and depending on that value, as well as the threats and risks to these assets, measures must be taken. Physical security measures are taken to protect information from fire, theft, vandalism, sabotage, unauthorized access, accidents and natural disasters.

Where does physical security start?

Physical security does not start at the workstation or workplace but outside the premises of the business. It has to be impossible to easily access the company assets that are to be protected. This can be illustrated simply and clearly by thinking in terms of a series of rings:

- Outer ring – Area around the premises;
- Building – The access to the premises;
- Working space – The rooms in the premises;
- Object – The asset that is to be protected.

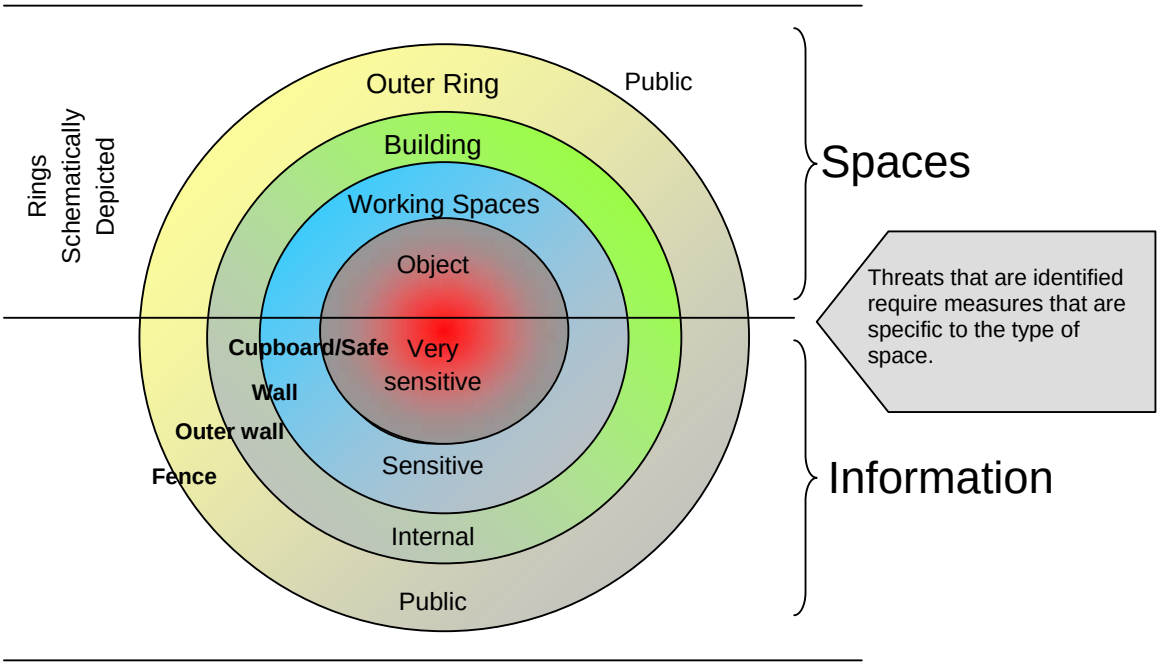


Figure 3: Protection rings

7.2.1 The outer ring

The outer ring that surrounds the business premises can be protected by natural and architectural barriers. Natural barriers can be, for example, thick vegetation or a river. Examples of architectural barriers include fences, barbed wire, and walls. All architectural barriers are subject to strict rules.

The outer ring must allow access to authorized persons, so barriers must always employ personal and/or electronic verification. These days there are many types of electronic sensors that are available, but we will not discuss these here.

The area between the outer ring and the business premises can be used for surveillance by a security guard and for auxiliary services such as, for example, parking, where the parking area is preferably screened off from the building. Such areas must have the appropriate lighting and possibly camera surveillance.

7.2.2 The building

There are situations where there is no outer ring. In these cases architectural measures such as windows, doors and other openings are important. It is, of course, best that these measures are taken whilst the premises are being built, as modifying an existing building can be very expensive.

Architectural measures are also subject to strict regulations. There are various ways of making openings in the premises secure; for example the use of break-resistant glass and doors with the correct frame and hinge mechanisms. The measures must be in line with the level of protection required by the organization.

In addition to the traditional locks, of which there are many types, in recent years increasing use has been made of electronic means to control access to buildings. Such means include card systems and code locks. Biometric equipment is still not commonly used. Biometrics refers to technologies that measure and analyze human body characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes. Biometric

characteristics can be divided in two main classes: physiological that are related to the shape of the body and behavioral which are related to the behavior of a person. In protecting the building, attention must also be given to the roof and walls. Cameras can again help with this.

7.2.2.1 Access management

There are various options available to manage the access to a business premises:

Electronic access management

Many organizations use pass systems with wireless RFID passes. These are currently the most widely used systems, but are being widely discussed as they can be 'tapped', copied and mimicked.

In the news

In more than half of the maternity wards in the American state of Ohio, both mother and child are given an RFID tag in the form of a wrist band or ankle band. In this way the wards hope to ensure that babies do not go missing, be abducted or given to the wrong parents.

Babies are given an ankle band whilst the mothers are given a wrist band. The HUGs system sounds an alarm if the ankle band breaks or if the RFID tag of the mother does not match that of the child.

Privacy protection organization *Consumers Against Supermarket Privacy Invasion and Numbering* (Caspian) has campaigned against this. They believe that HUGS will make hospitals less vigilant, as hospital workers would rely too much on the technology.

In addition to RFID passes, there are other sorts of passes that cannot be tapped.

When using access passes, a few complementary organizational measures are recommended:

1. Put a photo on the pass. This makes copying a little more difficult. Both the security system and the personnel are then able to check whether the pass belongs to the bearer;

2. Do not put the company name or logo on the pass, use a neutral design. If someone finds the pass, its purpose must not be obvious;

3. Require staff to wear the pass visibly. This should also apply to visitors, so that security and personnel can detect and approach anyone not wearing such a pass. Ensure that a system is set up whereby people who do not have a pass are escorted to the security staff.

For special rooms, vigorous authentication measures can also be used, where, in addition to the access passes, additional security measures are taken, such as:

1. Something that you know, for example a PIN code
2. Something that you have, for example a pass
3. Something that is part of you, therefore biometrics such as a fingerprint or an iris scan

Security guards

The use of security guards is the most expensive physical security measure. This measure can be supplemented by cheaper measures such as sensors and cameras that can be remotely monitored. In this case, there should always be a follow-up if an alarm were to go off.

It is best for the security personnel to also personally verify the access passes of those entering the building. This way it is harder to use fake passes.

7.2.3 The working space

Each working space may have its own particular function and so would be subject to its own security measures. For example, take a public building such as a town hall. We can enter the public areas of the town hall, but the offices are not accessible by everyone.

7.2.3.1 Intruder detection

In rooms on the ground floor and other special rooms, various types of intruder detection are possible. This depends on the type of room (size, type of wall, height, contents). The most commonly used method is passive infrared detection. Apparent motion is detected when an infrared (electromagnetic radiation) source with one temperature, such as a human, passes in front of an infrared source with another temperature, such as a wall. Of course, if the intruder detection system sets off an alarm, it requires an immediate response.

7.2.3.2 Special rooms

It is recommended that an organization set up special rooms and areas for suppliers to pick up and deliver goods so that they do not have access to the same business assets and information as the company's employees. The restriction of access is a preventive measure. There are a number of other important special rooms:

Storage of sensitive materials

Separate rooms can also be used to store sensitive materials. This can be information, but also medicines or expensive items. These rooms require extra measures to ensure their security. Access to special rooms must be checked, preferably by including these rooms in the access control system of the premises.

Server room

Server rooms and network rooms deserve a separate mention as they have to be approached separately when considering physical security. Server rooms and network rooms contain sensitive equipment that is vulnerable to humidity and warmth, and produce heat themselves. Also, an information system can stop functioning due to a power failure. One of the greatest threats to a server room is fire.

In addition to architectural requirements, server and network rooms also have special access control requirements.

Media such as backup tapes must not be stored in network rooms. It is best to store the tapes elsewhere, so that the tapes are not damaged in the event of a disaster. There's nothing worse than discovering after a fire that none of the information can be recovered because the backups have also been destroyed.

Cooling

In server rooms, the air has to be cooled and the heat produced by the equipment must be transported away. This air is also dehumidified and filtered. What often happens is that extra equipment is placed in the room without then adjusting the cooling capacity of the room.

In practice

 In an organization a cooling installation was placed in the server room many years ago. In the years that followed more equipment was placed in the room, but the cooling capacity of the room was not increased. Eventually the cooling system broke down, causing the temperature to rise. As a result, the servers failed, leaving the business without any central computer system for several days.

Emergency power

Equipment uses power, often a lot of power. In server rooms, it is advisable to use several independent power supplies. A number of other measures are used in addition to this:

- Battery packs or an Uninterruptible Power Supply (UPS) which, in addition to adjusting for dips in the power, filters the power and absorbs any peaks.
- Battery packs do not last forever, so it is wise to also have an emergency generator to provide power for outage longer than that battery can supply. The generator needs to be tested regularly and must be supplied with sufficient fuel for a sufficiently long period of time.

Power failures are a problem not only for computers but also production companies.

In the news

STEENWIJK, the Netherlands – On Thursday morning, households from some areas in the provinces of Overijssel and Drenthe were hit by a power failure. Households and businesses now have their power back. The power failure was caused by a fire that started at 8:40 in the morning in the main power station of the energy supplier in Steenwijk. It affected more than 10,000 homes and business. The residents were kept up to date on events by the police who drove around in sound trucks. Extra police had to be called in.

The management of a plastics company in Steenwijk is now experiencing problems with the continuity of its business. They are able to accommodate a dip in the power for a maximum of ten minutes, but after that the plastic begins to harden in the moulds and, in doing so, produces by-products that damage the moulds. The power had failed once before this week.

Some shops were not able to open, and those that did manage to open could only deal with payments manually and had to take cash. The stock inventory system could not be adjusted, which made the logistics planning a nightmare.

Humidity

Server rooms must not contain any moisture. For this reason, the air in these rooms is dehumidified. We must also ensure that no water pipes and central heating equipment have been fitted in the server rooms. These days it is possible to water-cool equipment, but such solutions must be inspected very carefully.

Fire

See also: Fire safety

Fire is one of the biggest threats that a special room, such as a server room or network room, can face. Certain measures are relevant here at all times:

- Smoke alarms to detect the smoke;
- Fire extinguishing equipment. If a fire breaks out, it must be extinguished quickly with the appropriate fire extinguishing equipment;
- No packaging material should be stored in these rooms. A server room is not a warehouse;
- Backup tapes should not be stored in the server room or the building itself;
- The cables used can be made extra fire-resistant.

7.2.4 The object

The “object” refers to the most sensitive part that has to be protected, the inner ring. Various options are available for storing and protecting sensitive materials:

Cabinets

A cabinet is the simplest way of storing things. It has to be possible to lock the cabinet, and the key must not be kept nearby. A cabinet is not particularly resistant against fire and can be relatively easily broken into.

Fire-resistant cabinets or security cabinets

A fire-resistant cabinet protects the contents against fire. Fire-resistant cabinets are available in various classes that indicate the degree to which they are fire resistant. Fire-resistant cabinets are not safes but they can also have burglary-resistant properties.

Fire-resistant cabinets are a good means for storing, for example, backup tapes, paper documents and money. It should be pointed out here that the backup tapes of a system must not be stored in the same premises as the information system. If a premises were to be completely destroyed, the tapes have to be still intact.

Fire-resistant cabinets or safes can be cemented in and can sometimes be entire rooms.

Fire-resistant cabinets or safes can have a variety of locks and protections against break-in.

7.3 Alarms

7.3.1 Sensors

Physical security uses various types of sensors. The most common are:

- Passive infrared detection. These sensors are usually used indoors and detect temperature changes within a certain distance of the sensor;
- Cameras. These sensors record images which can be viewed at a later time. Certain smart software allows automatic checks to be carried out;
- Vibration detection. These sensors detect vibrations;
- Glass break sensors. These sensors detect when a window has been broken;
- Magnetic contacts. These sensors detect when a door or window is opened.

7.3.2 Alarm monitoring

The sensors must be connected to an intruder detection system and should be well monitored. There are some systems that can even automatically contact an emergency center of a third party such as a security firm which is responsible for the monitoring. In any case, whenever an alarm is set off, the cause must be investigated. A logbook should be kept of all alarms.

7.4 Fire protection

Fire protection is a special area within physical security. There are compulsory fire protection requirements that must be met.

Fire is a threat that can always occur. Measures therefore must be taken at all times to protect against it. Fires can start in various ways, such as short circuits, defective boilers, human action, faulty equipment, etc. Fires require the following components: flammable material, oxygen and ignition temperature. This is the ‘fire triangle’. A fire can be combated using an extinguishing agent, the purpose of which is to break this fire triangle.

What sort of damage can be caused by fire?

- Damage by burning;
- Damage by heat;
- Damage by smoke;
- Damage by the extinguishing agents used.

7.4.1 Signaling

In order to signal the presence of fire, smoke alarms are usually used and are usually connected to a separate system. It is very important that the smoke alarms are checked regularly.

Organizations should regularly carry out fire and evacuation drills so that everyone is familiar with the sound of the alarm and the evacuation procedures.

7.4.2 Fire extinguishing agents

Fire extinguishing agents are aimed at combating one or more of the three components of fire, and, in doing so, put out the fire. There are different sorts of fires, and therefore also different methods of putting out these fires. Examples of various sorts of fires include: fire caused by electricity, chemical substances that burn or flammable liquids. The various fire extinguishing agents include:

- Inert gases (a gas that suppresses oxygen) such as: Carbon dioxide, Argon (noble gas), Inergen (brand name) and Argonite (brand name).
- Foam (water-based, not suitable for electricity);
- Powder (suitable for electricity, but damages metal);
- Water (not suitable for electricity);
- Sand (suitable for oil)

Below we can see the fire extinguishing installation of a server room.

7.5 Summary

The chapter on Physical Security covers quite a lot of ground. In essence, you have been introduced to the manner in which we try to protect our property.

We first determine who is allowed to enter our grounds, whereby we decide whether or not to place a fence around the area. If we do, how high does the fence have to be? Do we install cameras inside and outside the building? Is everyone allowed to walk around the building, or do we use access control systems inside the building as well?

As you have read, physical security is by no means just protection against theft. It also has to do with the cooling of machines. An overheated server will quickly break down, which would then affect the continuity. Protecting cables against any form of disruption means a better working environment.

Emergency power equipment ensures that we can continue working if the power were to fail (temporarily).

We have learnt that implementing only physical security measures is not sufficient to protect the Reliability of information. Physical security measures should be implemented together with complementary technical and organizational measures. These will be discussed in the following chapters.

7.6 Case study

A large pharmaceutical company is going to build a new location at an industrial park for clean industries. It will have a campus-like layout with a park structure. The buildings must appear fairly accessible to the public, but visitors must not be able to approach the buildings unseen.

The access to the buildings must be arranged in a friendly yet secure manner, so that people only have access to those parts of the buildings for which they are authorized.

The confidentiality of the information, for example the formula used, is a top priority. If third parties were to gain access to this information this could cause serious damage to the competitive position of the company.

Various zones will be introduced within the buildings: a public zone and various increasingly confidential zones. In the production area absolute hygiene is required, as everything there is free of dust. The air has to be continually purified and kept at the correct temperature, pressure and humidity.

The computerized systems are controlled by the company in its own computing center. This equipment is of great importance to the production process and for the development of new products.

You are given the task to formulate a watertight plan, in consultation with the architects and subcontractors, in which all the above requirements are met.

8. Technical measures (IT security)

Introduction

A risk analysis will suggest certain technical measures. The measures are in the area of physical security, which are usually also of a technical nature, as well as in the area of IT infrastructure security. This chapter will examine the security of the IT infrastructure and the protection of data against undesired access through access control and cryptographic applications.

We will also take a closer look at the correct use of an application and the correct processing of information. Information has to be reliable. After all, if we cannot trust that the information is correct and complete, it is of no use.

Although information systems are not necessarily computerized, we see in practice that computerized systems are playing an increasingly important role in information provision. As a result, the security of the computerized systems and the associated infrastructure is also playing an ever increasingly important role. IT security therefore is focused primarily on the security of the IT infrastructure. This chapter will examine the security measures that can be taken in the area of IT.

8.1 Logical access management

Logical access management is aimed at granting access to digital information and information services to those persons who are authorized, as well as preventing non-authorized people from gaining access to that digital information or service. The owner of the data, usually a manager, is the person who authorizes access during the authorization process. This authorization can be processed automatically by software, or can be granted by the system/application manager.

8.1.1 Discretionary Access Control (DAC)

With Discretionary Access Control, the decision to grant access to information lies with the individual user. An example of this is giving others access to one's own home directory. Another example is sending information to persons who do not themselves have access to that information. As this is a flexible form of access control, it is difficult to audit this and the information is difficult to secure.

8.1.2 Mandatory Access Control (MAC)

With mandatory access control, it is centrally determined and arranged which persons and systems have access to which information systems.

8.1.2.1 Granting access

In the granting of access, a distinction is often made between identification, authentication and authorization. Identification is the first step in the process to granting access. In identification the person or system presents a token, for example a key, username or password. The system then determines whether the token is authentic and to what resources access may be granted. As soon as this is determined, the authorizations can be allocated.

In practice

At the airport, I show the border guard my passport. The officer then checks the authenticity of this token by checking the authenticity features. For an information system, it is important that this check of the authenticity features (authentication) is unambiguous. A person can check the authenticity of a passport in various ways. He can, for example, compare the photo with the person's face. He could also check whether the photo fits the hole pattern on the holder page. In order to gain more certainty regarding the authenticity of the passport, however, he would have to consult a central administration system to check whether the passport has been withdrawn or stolen. The desired certainty about the authenticity of a token determines which checks have to be carried out before the token can be found to be authentic.

In the last step, the authorizations are granted. At the airport, to continue the example, I am granted authorization by being allowed to enter the departure terminal. This check is however insufficient to be authorized access to other parts of the airport such as the baggage handling section.

8.1.2.2 Security guards at access points

In addition to access control it is important to monitor who has access to what, and whether this authorization is abused. At the airport it has to be ensured that I do not try to gain access to areas for which I am not authorized. This guarding of access to certain areas can be for various reasons, such as restricting the risks as well as meeting certain statutory requirements. It may have to be shown that only authorized persons have access to certain information. This clearly shows that granting access is not only a technical matter, but that it is also an organizational concern.

In the news

In 2006, it was still something futuristic, but today the Dutch supermarket chain Albert Heijn and Equens have started a pilot whereby consumers can pay for their shopping using their fingerprint. The test will run for six months and will reveal what consumers think about this new payment method. "With Tip2Pay consumers can pay quickly, simply and safely by placing their finger on the scanner in the checkout lane." The fingerprint is linked to the address, bank account number and supermarket bonus card of the customer. At the end of the pilot, an evaluation will be carried out.

Source: www.security.nl

8.2 Security requirements for information systems

From the first moment that a company considers purchasing and developing information systems, it is necessary that security forms part of the project.

Information systems comprise operating systems, infrastructure, operational processes, ready-made products, services and applications that have been developed for the users. The design and implementation of the information system that supports the operational process can be a decisive factor in the way the security is set up.

Security requirements need to be agreed upon and documented before the information systems are developed and/or implemented.

When security requirements are documented during the risk analysis and specification of the requirements for the project, they are justified, agreed upon and documented as part of the total 'business case' for an information system.

It is considerably cheaper to implement and maintain security measures during the design phase than during or after the implementation.

In practice

A large organization has a new intranet developed. Two weeks before it is launched, the Information Security Manager (ISM) is asked whether she can have a look at the security measures. A thorough investigation brings to light so many vulnerabilities that the intranet has to be completely redesigned, which results in more than a year's delay in its launch. Many hundreds of thousands of Euros in company resources are wasted as a result of poor communication!

When buying a product, a formal test and purchasing process should be followed. The contract with the supplier must state the requirements that the product's security has to meet. If the security functionality in the product does not meet the requirements, then the resulting risk and the associated security measures will have to be reconsidered; as well as the question of whether or not to buy the product.

8.2.1 Correct processing in applications

Applications (software, computer programs) must work as intended. A program that causes errors, allows data to be lost, enables unauthorized persons to make changes or misuse information, is a large risk.

Application systems and applications that have been developed by the user should incorporate suitable management measures. Such management measures concern the validation of the data that is entered, the internal processing and the output data. This means that the information has to be entered in such a manner that the data can be checked to see whether it is correct.

In order to simplify the input of data, master tables and terminology lists are often used. These lists, which are built into the software/database, can prevent more than one word being used for a single term.

In practice

A policeman observes an accident and records it in the system: pedestrian on the pavement is hit by a moped.

The following day another policeman observes an accident at the same location and records it in the system: a walker on the footpath is hit by a scooter.

If the database is later examined for a study into dangerous traffic situations the correct information will not be given.

The system must force the use of only selected words such as pedestrian, pavement and moped and not accept words such as walker, footpath and scooter. When a search is then made according to the correct words, all accidents that meet those criteria will be produced by the system.

8.2.2 Validation of input and output data

Data that is entered into applications should be validated in order to ensure that it is accurate. Business transactions and fixed data can be checked automatically. Consider, for example, an input field for the postal code that always has a fixed format. This applies just as well for sale prices, exchange rates, tax rates and credit limits.

Validation is an important tool to protect against mistakes and misuse from users.

8.3 Cryptography

Remark: *Sections 8.3, 8.4 and 8.5 elaborate on cryptography. To pass the EXIN exam: Information Security Foundation based on ISO/IEC 27002, the candidates need to understand the concepts 'cryptography', 'digital signature' and 'certificate' without technical knowledge about how they work.*

The term cryptography comes from the Greek, and is a combination of the words kryptós which means 'hidden' and gráfo which means 'writing'. Examples of cryptography are as old as the proverbial road to Rome. It was actually used by the Romans to convey military messages. Even if the message were to fall into enemy hands, they would not be able to derive any information from it as the message would appear meaningless. Research into cryptographic algorithms is also referred to as crypto analysis and is used not only to develop algorithms but also to crack the algorithms of enemies. Crypto analysis made particular advances in development during and after the Second World War.

Cryptography is often seen as a means to keep information secret. However, it has other applications, such as protecting the confidentiality, authenticity and integrity of information.

In the news

A student from the Radboud University in Nijmegen, the Netherlands, has succeeded in making a machine costing only forty Euros that is able to copy a disposable version of a public transport chip card. This copy can be used repeatedly as a transport ticket.

The student electronically listened in on the communication between an original disposable card and the chip reader at a gate. It turned out that the information sent by the disposable card was not encrypted; unlike that sent by the subscription version of the card which is registered under the name of the subscriber. It seems that for the disposal version, a chip with encryption is too expensive.

Source: www.computable.nl

8.4 Cryptography policy

Cryptography is a measure that an organization can employ if, for example, confidential data is involved. The use of cryptography has to be carefully considered and defined in a policy document.

This document should contain the following:

- What does the organization use the cryptography for;
- What types of cryptography does the organization use, and in which applications;
- Control and management of keys;
- Backup;
- Control.

8.4.1 Key management

The management of the key is an important part of the policy in the use of cryptographic techniques. Cryptographic keys should be protected against alteration, loss and destruction.

What's more, secret and personal keys have to be protected against unauthorized disclosure. Equipment being used for generating, storing and archiving keys should be protected physically. Part of key management is the registration of the key pairs. Which pairs have been issued to whom and when. Until when will the keys be valid? What must be done if the keys are compromised?

It is a great risk to use the same keys on various equipment within an organization. If these keys become known outside the organization, then the equipment (often laptops) will have to be provided with new keys. This can be a very expensive operation which would have to be carried out very quickly.

8.5 Types of cryptographic systems

In order to be able to make use of a cryptographic system, both the sender and recipient must have the algorithm. A characteristic of a good cryptographic system is that the algorithm itself is public. Generally speaking, there are three forms of cryptographic algorithms: symmetrical, asymmetrical and one-way encryption.

The algorithm has to be able stand the test of criticism and should be open. The more people that look at it, the more difficult it will be to penetrate. The keys are the secret component of the cryptography.

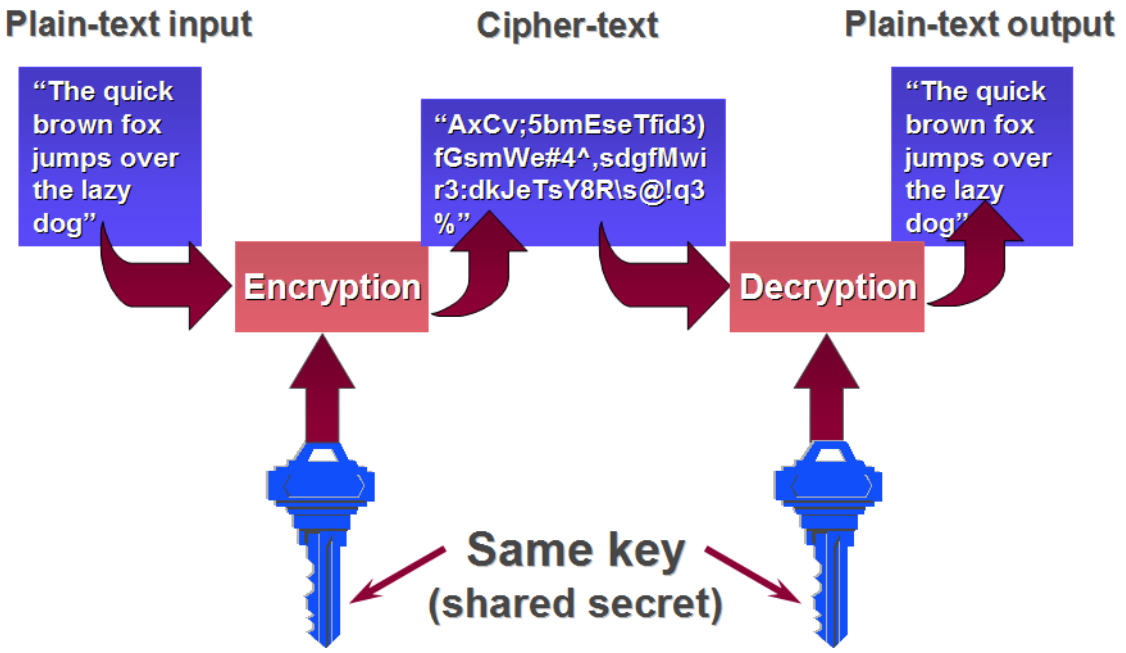
The Public Transport chip card in the Netherlands contained a secret algorithm and a certain number: These were weaknesses. If the design of the myfare chip had also been publically scrutinized by scientists, it would never have been publically released in such a way.

8.5.1 Symmetrical

Everyone probably knows some form of symmetrical cryptographic system. A characteristic of such a system is that there is an algorithm and a secret key that the sender and recipient share.

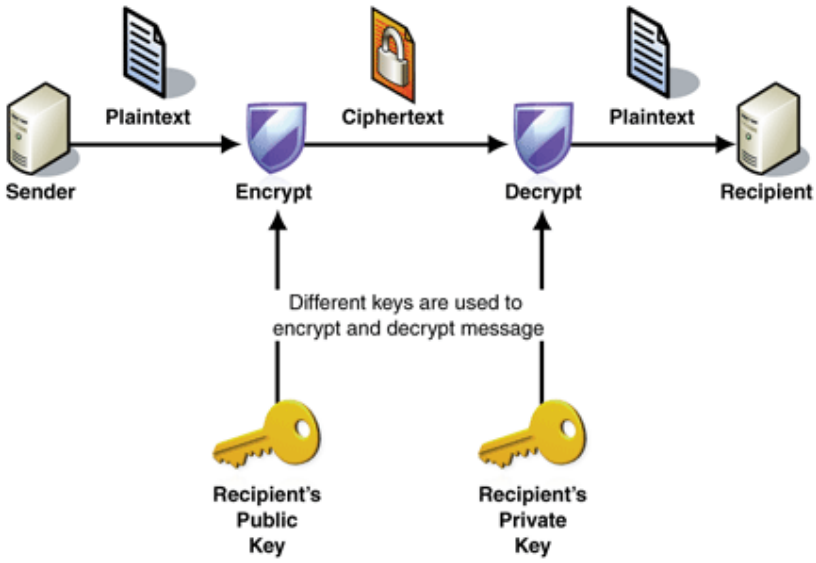
In practice

A simple way of encrypting a message is to shift the letter along the alphabet by x places. If x=+5 then 'A' becomes 'F'. Everyone who knows the secret key will be able to decode the message by shifting the letters by x=-5 along the alphabet. As this example illustrates, the secret key can be used to both encrypt and decrypt the message. The strength of this cryptographic system depends directly on the ability of both the sender and recipient to keep the shared key a secret.



8.5.2 Asymmetrical

An asymmetrical system solves the vulnerability involved in sharing a secret key. The characteristic of an asymmetrical system is that different keys are used for encrypting and for decrypting. This system was conceived in 1970 by Ron Rivest, Adi Shamir and Len Adleman and works on the basis of prime numbers and modulo mathematics. The most striking aspect of this algorithm is that it is no longer necessary for the sender and recipient to have the same key. The algorithm works with so-called key pairs. Using this method, the private key is responsible for the encryption and only the public key of this key pair can decrypt the message. What makes this system so special is that the public key can be known to the whole world.



This system can be used in two ways. The first way is to sign the message with the private key. Using the public key the recipient can verify whether the message has originated from the owner of the relevant private key. The second way is to encrypt messages intended for a person with their own

public key. Only the holder of the private key associated with this public key will be able to decrypt this message. Please note here that the use of the private key is restricted to the holder of the private key, whilst everyone can make use of the public key. In this way asymmetrical algorithms can be employed to guarantee both the integrity and confidentiality of messages.

Digital signature

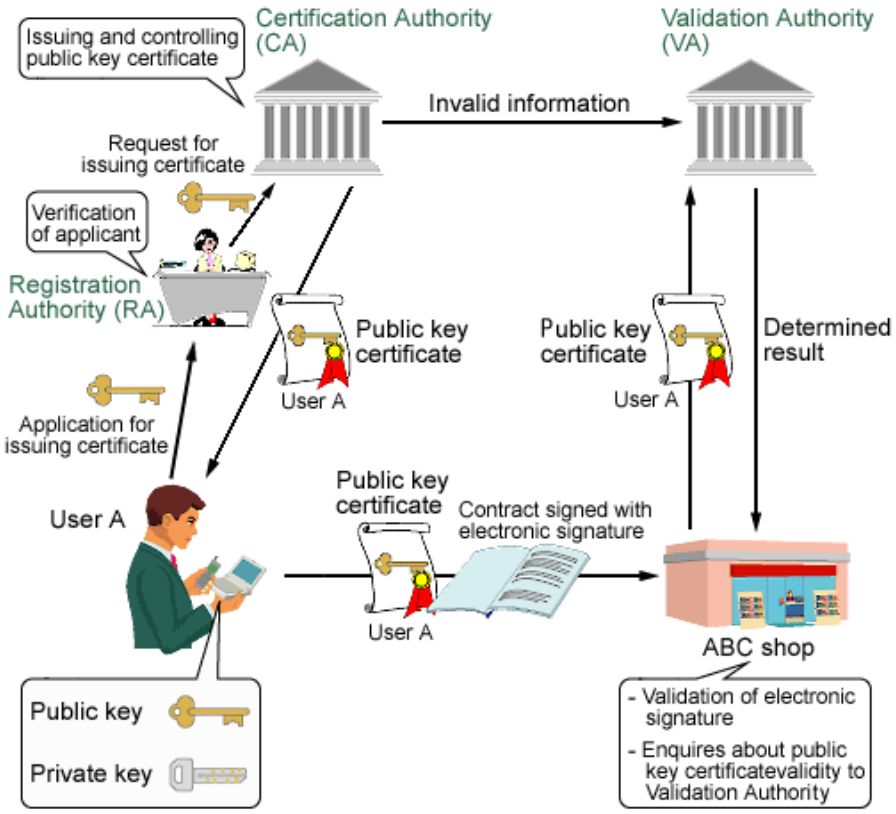
Digital signatures are created by using asymmetrical cryptography. A digital signature is a method for confirming whether the digital information was produced or sent by whom it claims to be—comparable with signing paper documents with a written signature. A digital signature generally consists of two algorithms: one to confirm that the information has not been changed by third parties, and the other to confirm the identity of the person who has “signed” the information. In Europe, thanks to the Directive 99/93/EG, a digital signature is now regarded as equal to a “paper” signature. In most cases, it has to be possible to verify this digital signature using an attested certificate which must be made through secure means (for example a smartcard).

8.5.3 Public Key Infrastructure

Asymmetrical cryptography is also referred to as Public Key Cryptography. Please note that this is not the same as Public Key Infrastructure (PKI). With a PKI much more is involved. A characteristic of a PKI is that through agreements, procedures and an organization structure, it provides guarantees regarding which persons or system belongs to a specific public key. A Public Key Infrastructure is often managed by an independent authority. Vecozo is a Dutch example of such an authority. Vecozo ensures the exchange of confidential information in the health care sector.

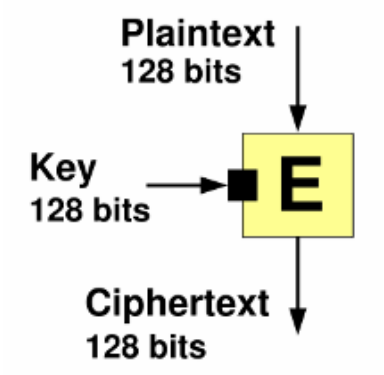
In practice

A family doctor wishes to make a declaration of her treatments electronically with the medical insurance companies. The medical insurance companies have a contract with a Certification Authority (CA). The family doctor requests a certificate from the CA. The CA is responsible for confirming whether the family doctor is who she claims to be, for example by requesting her diplomas and a signature. The family doctor is given access to the website in order to download the certificate. This is a file that is downloaded onto the computer. If the family doctor wants to make a declaration, she goes to the website of the CA. When logging in, the certificate on her PC is checked; the username and password associated with the certificate are requested. She is then given access to upload her declaration files. Which are digitally signed as being genuinely from her. She can also, for example, check whether a particular patient is insured and through which medical insurance company.



8.5.4 One-way encryption

This form of encryption is also called a hash function and can be compared to mixing paint. As soon as two colors of paint mix with one another it is impossible to separate them. This type of algorithm is chiefly used to determine whether certain data has changed. The message is converted into a numerical value. Using a known algorithm, the recipient can check whether the message has the correct hash value; if the two hash values match, the message must be unchanged. Hashes can also be used to confirm that two messages, passwords for example, are the same. When a password is set, the system makes a hash and then stores that hash value *not* the password itself. This way, even a person with high-level access to the system cannot see what the person used for a password. Later, when the person presents the password for authentication, the system again takes a hash of the password and compares it to the hash stored in the system. If the hashes match, the person must have entered the correct password. This method is used to check the integrity of messages, it does not provide confidentiality.



8.6 Security of system files

8.6.1 Access management for program source codes

System files lie at the heart of the computerization of an organization. If the source code of these files fall into the hands of someone with malicious intent, it is possible for that person to gain access to confidential information. These files must therefore be treated with the utmost care.

Access to the source code of programs must be restricted to only those who have a genuine need for this access.

8.6.2 Security of test data

It is important that equipment and program test data be carefully chosen, protected and managed. Real data, which could contain sensitive information such as personal details, must not be used for testing. Test systems must only use fictitious data.

8.6.3 Security in development and support processes

Managers who are responsible for application systems are responsible for both the security of the project environment in which the applications are developed and the environment in which the applications are supported. They also determine whether proposed changes could jeopardize this security.

8.7 Information leaks

It is possible for information to leak out through **hidden communication channels**. It would be unlikely for the average employee to be aware of the presence of such a communication channel. Secret communication channels are channels that are not intended for processing information, but nonetheless can exist in a system or network. It is difficult, if not impossible, to prevent all possible secret communication channels. The use of such channels is a common feature of trojans (see also the chapter on Malware). It is possible that the supplier of a custom-made program leaves a secret access method in order to carry out maintenance in the application, without informing the buyer of this. This is referred to as a maintenance door or a back door. This practice is not normally appreciated by customers. When the custom-made application is used for processing highly confidential information, an independent bureau can inspect the source code of the application for such secret communication channels.

8.7.1 Outsourcing program development

When the development of computer programs is outsourced, it is important that this development is supervised and controlled by the commissioning organization.

Who becomes the owner of the source code? If possible, the client must have the intellectual property rights.

The quality and precision of the work that has been carried out can be determined through certification by an independent body. Consider for a moment the discussion above regarding the monitoring of the hidden communication channels.

8.8 Summary

Access to buildings is controlled as is the access to the network infrastructure. How do we deal with the access rights provided to staff in the IT environment? The rights given to one member of staff can differ from those given to another. How do we determine who is allowed to do what? When that has all been determined, it is then time to distribute the available information to the employees who are permitted access to the particular systems. This is done through access control.

When information has to be effectively protected against access from unauthorized persons, we use cryptographic applications. You have been introduced to cryptography and now know the difference between symmetrical and asymmetrical cryptography and PKI solutions.

8.9 Case study

A medium-sized bank has plans to greatly expand the IT environment. The management board has decided that it is necessary to replace all IT facilities with new equipment. Open source is being considered. It is important that all the new hardware is provided with good support. The current computer program that was specifically designed for the bank is no longer adequate. The IT department is now going to develop new programs that can be used flexibly on various Operating Systems (OS). This development may be outsourced.

This bank employs large numbers of staff who work in a limited number of areas. There are differences in authorization levels. Only a small number of staff have access to strategic information such as the annual figures and the financial administration. These staff do not, however, have access to customer data, again showing the many separate levels of authorization.

All stored data must, of course, be protected against unauthorized access. What's more, the exchange of certain sensitive data with external parties must be encrypted.

It is important that the new system has means to ensure that only the correct information may be entered. Entries, depending on the amount, are subject to various controls. Very large amounts are checked by more than just one person.

You are given the task of setting up a study into the security of the new network and computer systems that are to be purchased. Do you opt for normal PCs or will you decide upon a thin client principle? Explain your decision. Which OS will you choose and why?

How will you arrange the authorization structure? What techniques will you use to determine the various levels?

Will you choose to have your company carry out the software development or will you use an external company? Give the advantages and disadvantages of both options and indicate the possible pitfalls for the bank.

In this case, there are many considerations that have to be taken into account. Describe these considerations and explain your choices.

9. Organizational measures

Introduction

In the previous chapters, we took a closer look at the physical security of the work environment and the technical security of the IT infrastructure.

This chapter will examine various organizational measures. Organizational security measures are often inextricably linked with technical measures. When relevant, we will refer to the technical measures that are necessary in order to be able to carry out or enforce these organizational measures.

We will, for example, take a closer look at (security) policy, the PDCA cycle and the components of ISO/IEC 27001 and 27002, an important international standard for information security. We will also discuss the organization of information security and the way in which information security can be propagated in the organization.

How do we deal with disasters? What are disasters exactly and how do we prepare for them?

If a disaster were to occur, what procedure will be followed in order to ensure the security of people and other assets and to get back into operation as soon as possible?

We will also examine communication and operational processes, test procedures and the management of the IT environment by an external provider.

9.1 Security policy

9.1.1 Information security policy

By establishing a policy for the security of information, management provides direction and support to the organization. This policy must be written in accordance with the business requirements as well as the relevant legislation and regulations.

The information security policy should be approved by the management board, and published to all staff and all relevant external parties, such as customers and suppliers.

In practice, the latter is usually carried out as a summarized version of the policy outlining the main points. This can be in the form of a flyer issued to all staff and included as part of the introduction of new personnel. The complete version can be published on the intranet of the company or in some other location that is easily accessible to all staff.

In the news

At Virgin Media, the entertainment branch of Richard Branson's Virgin Group, a CD containing the names of 3000 customers has been lost. The unencrypted disk contains the bank details, names and addresses of three thousand customers who have arranged memberships at various shops since January. The data was placed on a CD in violation of company policy.

9.1.2 Hierarchy

It is common for a policy document to have a hierarchical structure.

Various policy documents are developed with the high-level corporate policy as basis. They must always conform to the corporate policy and provide more detailed guidelines to a specific area. An example of this is a policy document on the use of encryption means.

The following items may then be written with the policy documents as basis:

Regulations. A regulation is more detailed than a policy document;

Procedures describe in detail how particular measures must be carried out, and can sometimes include the work instructions, for example a clear desk policy. In order to ensure that sensitive materials cannot be easily removed, a clear desk policy is necessary. No information should be left unattended on a desk, and after working hours all information must be stored in something that can be locked.

In practice

Within the general encryption policy there may be a procedure on how to deal with a particular encryption means. This would therefore be compulsory. The procedure would then explain how the user is to handle the encryption software and the key itself.

A procedure can also define how the system manager is to install the encryption software. These instructions are very detailed, such as what boxes need to be checked, the number of characters a password requires and for how long the password remains valid.

Guidelines, as the term suggests, provide guidance. They describe which aspects have to be examined with particular security aspects. Guidelines are not compulsory, but are advisory in nature;

Standards can comprise, for example, the standard set up of particular platforms.

In practice

A guideline provides advice on the requirements that a classification policy has to meet. The staff responsible is then free to choose the way in which he or she will carry out the classification policy for the organization.

An important example of a standard is ISO/IEC 27001:2005. This is a standard for setting up information security in the organization. Part I, ISO/IEC 27001, describes the management system (Information Security Management System, ISMS). Part II, ISO/IEC 27002:2005, which is also called the Code for Information Security, develops this management system through practical guidelines. An organization can have itself certified for ISO/IEC 27001:2005 and consequently show suppliers and customers that it meets the quality requirements for information security. The Code for Information Security is suitable for all organizations, small or large, government or businesses.

9.1.3 Evaluating the information security policy

The information security policy is one thing, implementing it in the organization and checking whether it is being adhered to, is another.

Many organizations work with the PDCA cycle (see figure in section 9.1.4).

The information security policy is the main document. The information security policy includes policy documents, procedures and guidelines that are aimed at a certain aspect of the information security and which provide detailed expectations. These documents are an important part of the Information Security Management System (ISMS).

9.1.4 PDCA model

The PDCA model, also called Deming's quality circle, is used as a basis for determining, implementing, monitoring, controlling and maintaining the Information Security Management System (ISMS).

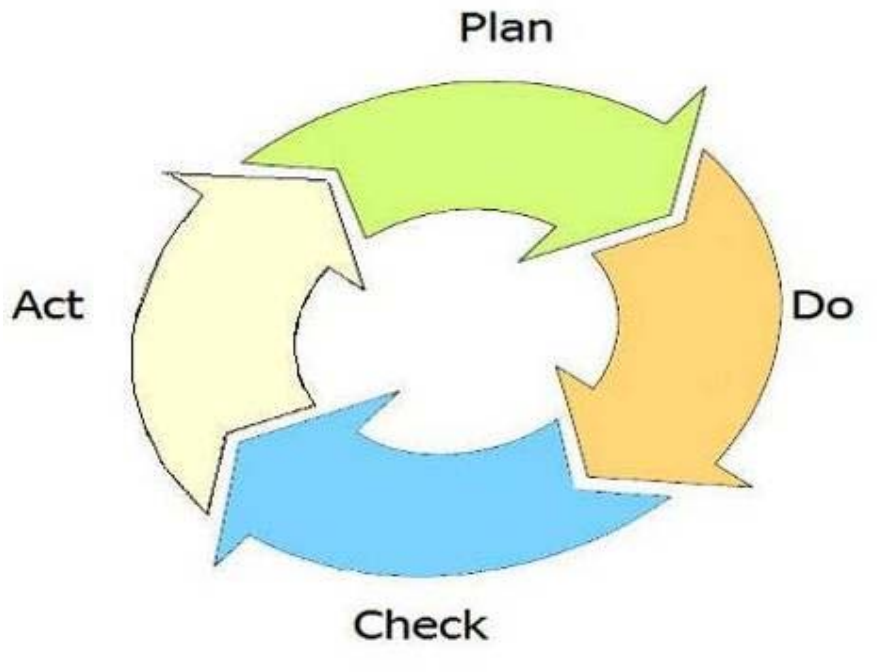


Figure 4 - PDCA model linked to the ISMS processes

Plan (design the ISMS)

In the design phase, an information security policy is developed and documented. Here the information security objectives, the relevant processes and procedures are defined that ensure that the risks are managed. These objectives must, of course, support the business objectives of the organization.

The security measures can be taken on the basis of a risk analysis and a cost/benefit analysis. There are other methods, but we will not go into them here.

The Plan phase applies not only to the main policy but also to all supporting policy documents and underlying regulations.

Do (implement the ISMS)

In this phase, the information security policy and the underlying procedures and measures are implemented. Responsibilities are allocated to each information system and/or process.

Check (monitor and check the ISMS)

In this phase, controls are carried out using self-assessment (internal auditing) and, where possible, measurements are carried out to see whether the information security policy is being correctly executed. A report on this is issued to the management responsible and the Chief Information Security Officer (CISO).

Act (maintain and adjust the ISMS)

In this last phase, corrections are carried out and preventive measures are taken, based on the results of the internal audit. When necessary, the ISMS is updated.

The PDCA cycle is a continual cycle. This is described in an ISMS manual.

9.1.5 Setting up ISMS

The organization formulates a framework for the control of its ISMS.

This framework provides a logical classification of all the matters relating to information security by arranging them into domains.

A domain is a group of subjects (clusters) that are logically connected to one another. Domains form the basis to the ISMS framework. Many of these clusters produce their own policy documents, procedures and work instructions.

The ISMS comprises at least the eleven domains as identified in the ISO/IEC 27002 standard. These are in line with the processes for IT Service Management as described in the ISO/IEC 20000 standard.

9.1.6 The eleven domains in the ISO/IEC 27002

A.5 Security policy

A.6 Organization of information security

A.7 Management of assets

A.8 Security of personnel

A.9 Physical security and security of the environment

A.10 Management of communication and operating processes

A.11 Access security

A.12 Acquiring, developing and maintaining information systems

A.13 Management of information security incidents

A.14 Business continuity management

A.15 Compliance

The domains listed above start from A.5 as these numbers correspond to the chapters of the ISO/IEC 27002. The first 4 chapters give an introduction to the eleven domains.

Each domain has a number of sub-domains. For example, access security comprises both physical access and logical access.

A domain is described in a policy objective and is worked out in further detail in underlying guidelines, procedures and aids.

9.1.7 Monitoring information security policy

The information security policy is regularly assessed and, if necessary, modified. The permission of the management board is required for any changes to the policy.

9.1.8 The organization of information security

Without effective security of information, it is not possible for an organization to survive. Everyone in the organization must accept this and the management board and management have to act as examples. Only when they themselves support their own policy, will the staff take information security seriously and so work to comply with the measures.

Information security is a process in which many people are involved. The process needs to be controlled effectively. If there is no responsibility or management, then information security will not be effective. The manner in which information security is managed depends on the size and the nature of the organization. In small organizations, information security can be just one of the responsibilities of

several people. A self-employed person without any employees is responsible for all aspects of information technology, including security. In contrast, in large organizations, there will be personnel whose sole responsibility is a particular aspect of information security.

In the information security process, periodic consultation needs to take place between all those with primary responsibility. In addition to the information security officers, these can also be personnel who are responsible for implementing certain measures. These are preferably people who work in the Human Resources, Information, Finance, Accounting or Accommodation departments.

9.2 Personnel

See also: Segregation of duties in section 9.4.3.

Personnel can also be regarded as business assets. People and their knowledge and skills are valuable assets, and measures are necessary to protect this value.

All personnel are responsible for information security. This responsibility must be made clear in the employment contract. The staff manual can contain a code of conduct and the sanctions that are imposed in the event of non-compliance and if incidents arise as a result. The code of conduct may state, for example, that private e-mails are not permitted. The manager is responsible for the correct job descriptions and is therefore responsible for the various aspects related to dealing with information in the various positions.

When a person applies for a job which involves working with sensitive information, references, identity and diplomas must all be checked. If a person has committed a criminal offence, this can be brought to light by making it compulsory to fill in a ‘certificate of good character’ or requiring a fingerprint-based background check. These certificates are issued by the Department of Justice and can be requested from the city hall. Background checks may be arranged through the local law enforcement office and should have a scope beyond just the local area. For example, a check for criminal offense in the U.S. should be run across all 50 states not just in the local County or State.

The organization must have rigorous procedures for when personnel leave and enter employment or when they change jobs within the organization. It must not be forgotten to change or remove rights, collect equipment and passes. Access rights must be controlled regularly.

9.2.1 Screening and Non Disclosure Agreement

For a position involving confidentiality, this confidentiality may have to be observed even after the employment ends. The manager is responsible for documenting special rules for specific positions. In every case, all personnel with a position that involves confidentiality must sign a Non Disclosure Agreement (NDA). It is also usually the case that these personnel have to submit a certificate of good character or background check.

They may also have to undergo a screening or security examination. How in-depth this screening is, depends on the level of confidentiality associated with the position in question. Take, for example, security guards, managers and financial staff. Screening is very expensive. The government has organizations that conduct such screening. Businesses can sometimes use such organizations if they carry out work commissioned by the government. However, there are also private organizations that carry out these screenings.

9.2.2 Contractors

The security requirements that apply to the personnel of an organization also apply to any staff the organization may hire on a temporary basis. The written agreements with the supplier, such as a recruitment agency, must include sanctions in the event of violations.

9.2.3 Personnel files

Personnel data and personnel files must be handled confidentially and be well stored. It should also be documented who is allowed to have access to these personnel files.

A personnel file contains information such as the job profile, the employment contract and various signed declarations. A code of conduct for computer use is an example of such a declaration. Other examples include a code of conduct for e-mail use, declarations of understanding and intention to observe legislation (for example in the area of data protection and computer criminality) as well as a Non Disclosure Agreement.

9.2.4 Security awareness

One of the most effective measures for information security is that personnel have to attend a security awareness course when entering employment. This course can be part of the introduction and the internal training.

In order to support information security awareness, various means can be used: flyers, booklets, messages on computer screens, mouse pads, newsletters, videos and posters.

Large organizations often arrange separate security awareness courses for people such as system managers, developers, users and security personnel. Other groups may also benefit from a course that is specific to their own particular work.

These courses and campaigns focus particularly on the company rules regarding information security and the anticipated threats.

Security documentation and information must be available to everyone in the organization. Different documentation is often produced for different target groups (users, managers, developers, etc.). The documentation needs to be revised on a periodic basis, but also when there have been changes or when any new threats appear.

Staff must be made aware of the importance of not allowing company information to get out in the open. Everyday social activities and contacts such as birthdays, clubs, friends and, in particular, casual acquaintances, form a risk. Information tends to be more easily shared in a relaxed atmosphere, which may then lead to it getting into the wrong hands.

Social engineering is an example of a conscious attempt to extract confidential information. Someone may try to gain the confidence of an employee by pretending to be a colleague or a supplier, but is really trying to acquire confidential information. In a large organization where not everyone knows one another, there is a good chance of success. The social engineer takes advantage of people’s weaknesses. When, for example, we hear someone speak using the correct jargon, we assume that he is part of the organization. Of course, the social engineer may have simply heard these terms in the café.

In the news

Around February 14, thousands of computer users received an e-mail that was infected with malware.

Mail users receive an e-mail containing a large heart with the invitation to click a hyperlink with an IP address. In so doing computers are infected with a trojan, allowing the system to be included in a network of infected PCs. This so-called 'botnet' can be remotely controlled by cyber criminals and be used to commit crimes. One example is to establish fraudulent bank websites that mimic the bank's real website.

Earlier during Christmas and New Year, a batch of infected e-mails were sent. The Storm Worm is one of the most stubborn threats in the history of the Internet.

9.2.5 Access

For large organizations where not everyone knows one another, a good access control system is of even greater importance. An example of this is a system whereby both staff and visitors have to wear clearly visible passes.

All visitors have to be registered on arrival and departure. All access is recorded, visitors check in and out at reception, and write down their arrival and departure time. An employee who is expecting a visitor can also check-in the visitor and escort the person around the building up to the moment of departure.

9.3 Business continuity management

We cannot be prepared for everything. Floods such as those of Spring 2007 in England and the Autumn floods in Bangladesh in 2007 caused great losses to the countries' economies. There was the enormous damage caused by hurricane Katrina in New Orleans. Terrorist attacks in New York, London and Madrid, as well as simple power failures lasting several hours, can have considerable consequences for the availability of people and systems within a company.

Each year, companies all over the world are hit by disasters that have a huge impact on the availability of their systems. Only a small percentage of these companies prepared themselves for these eventualities. The majority of companies affected by such huge disasters do not normally survive them. The companies that do survive this sort of disaster have carefully thought about these eventualities in advance and have documented and followed the necessary measures and procedures to protect themselves.

An organization is dependent upon assets, personnel and tasks that have to be carried out on a daily basis in order to remain healthy and profitable. Most organizations have a complex network of suppliers and assets that are dependent upon one another in order to be able to function. There are communication channels such as telephone and network connections, and there are buildings in which work is carried out. The buildings have to be in optimum condition in order to ensure that the work is not only pleasurable but also carried out efficiently.

If a link in the chain of dependencies fails, this can lead to problems. The more links that fail, the greater the problem. And the longer certain components in the chain are out of action, the greater the effect this has on the organization, and the longer it will take to restart normal operations.

Thinking in advance about the continuity of the work processes is essential for an organization. It does not matter whether this is a complex production process or a relatively simple process such as the processing of residents who have moved to a new house. For both the personnel and the customer, it is important that each component, big or small, of the process works smoothly, and continues to do so in the event of difficulties.

The purpose of Business Continuity Management (BCM) is to prevent business activities from being interrupted, protect critical processes against the consequences of far-reaching disruptions in information systems and allow for speedy recovery.

In the management process of business continuity, the business processes that are critical to the operation of the organization must be identified. In addition to other measures that ensure the continuity, the loss of information that could arise as a result of a natural disaster, an attack, fire or power failure, must be avoided. The consequences of disasters, security incidents and the failure of services are assessed in a Business Impact Analysis (BIA). The continuity plan describes how information required by the critical business processes can be quickly made available.

In information security, continuity management is usually split into two separate, but closely related, components:

Business Continuity Planning (BCP) in which the continuity of the business processes is guaranteed;

Disaster Recovery Planning (DRP) whereby the recovery after a disaster is organized.

Business continuity management is described in the BS 25999, which is a British standard comparable with an ISO/IEC standard.

ISO/IEC 27002 includes some BCM measures, but these are primarily aimed at the Information component, while the BS 25999 is applied integrally throughout an organization.

9.3.1 Continuity

Continuity concerns the availability of information systems the moment that they are required. Various requirements can be imposed upon this availability. Do you have a telephone exchange where fifty staff are on the telephone twenty-four hours a day? Then you would undoubtedly have different availability requirements than a company with only one person on the telephone who receives a telephone call only once every hour.

For a city council, the availability of the municipal database is of great importance. If this were no longer available, then large numbers of staff would not be able to carry out their work. However, if this system were not available to the council at night, then this would pose no problems.

We can see here that, depending on the organization, the field of work and even the division within an organization, availability requirements can differ dramatically.

9.3.2 What are disasters?

We will now take a closer look at what we mean by disasters. On the face of it, a disaster sounds quite threatening. But nothing is further from the truth. In this context, the failure of a simple system could already be regarded as a disaster. A disaster does not necessarily have to be a flood or a terrorist attack. The failure of the system upon which you depend so much for your daily work, through a technical problem, is also a disaster.

In practice

A simple network card in the mail server that becomes defective can be an utter disaster. These days, staff would not be able to carry out their work properly if deprived of their e-mails.

How does your company respond to a disaster?

The consequences that a disaster may have on a business depend on the nature of the disaster. If the work has been disrupted due to a failure of a system or the complete network on which the office IT operates, then a telephone call to a service desk or helpdesk is often enough to get the necessary activities back and running.

If the health of an employee is being threatened, then a telephone call to the in-house emergency service or national emergency number would be the correct action.

In all cases, human life has priority over software and equipment. The evacuation activities have to be set in action first, only then should attention be given to the business processes, starting with the most crucial to the business.

It is important that there be effective and clear procedures that define which actions have to be taken, for example:

- You know that, in the event of an information system failing, you have to contact the helpdesk;
- You know where the emergency exits are in the building;
- You know who to phone in the event of a fire, the spontaneous setting off of the sprinkler system or a bomb alert.

The helpdesk or in-house emergency service worker must know what to do for each type of alert. They will have a priority list which documents who and what has to be helped and when, as well as which organizations they have to contact for each different alert.

The training of in-house emergency service workers is very important. In-house emergency service workers are normal personnel who have decided to take on these additional duties. Ensure that there are in-house emergency service workers throughout the entire organization.

Bomb alert

A bomb alert is not normally regarded as a risk for an organization. They are not a normal occurrence in most countries. However, in the last few years people have become more aware of suspicious packages. It is therefore advisable to have procedures in place for this as well. The bomb alert procedure must clearly describe what to do in the event of someone raising an alarm. Suspicious items can enter any company. Personnel must know what is not normal and be able to identity suspicious items. Attention should be given to this during the security awareness campaign.

9.3.3 Disaster Recovery Planning (DRP)

What is the difference between Business Continuity Planning and Disaster Recovery Planning?

The purpose of DRP is to minimize the consequences of a disaster and to take the necessary measures to ensure that the staff, business assets and business processes are again available within an acceptable time.

This is different to BCP, in which methods and procedures are also arranged for failures that last a longer period of time.

A DRP is aimed at recovery immediately after a disaster. The DRP is put into action when the disaster is still ongoing. Work is focused on determining the damage and getting the systems running again.

A BCP goes further and has a wider focus. BCP arranges an alternative location where the work can be carried out while the original location is rebuilt. In BCP, everything is focused on keeping the company running, even if only partially, from the moment the disaster occurs up to when the company has fully recovered.

In other words:

DRP: There is now a disaster and what do I have to do to get back into production;

BCP: We have had a disaster and what do I have to do to get the situation back to how it was before the disaster.

In practice

An employee uses an *intranet* version of the telephone directory. This suddenly fails so she informs the helpdesk of this. The employee can however continue her work by simply using the *internet* version of the telephone directory.

Such a message to the helpdesk will not receive high priority.

An IT employee is working on recovering the intranet telephone directory. A message comes in that an important system has failed, resulting in the production process coming to a standstill.

Everyone understands that the continuity of such a system will receive higher priority than the recovery of a system for which there is an alternative.

When developing a BCP and/or DRP, a variety of solutions can be considered for getting the business processes running again. If it is decided that, in the event of a disaster, the business processes and systems must be made available as soon as possible, the best option is to develop plans and procedures for a stand-by arrangement. Such arrangements must be tested regularly. The plan also needs to include how the stand-by arrangement, once activated, will be withdrawn; it must be clear under what conditions normal operations may be resumed.

Alternative workplaces

A large, well-known Dutch bank has, through an inventive use of many different locations, ensured that its staff would be able to carry on working in the event of a disaster. Certain key players in the organization have been assigned alternative workplaces in another branch. If something were to happen at the permanent workplace of these key players, he or she would travel a few kilometers to the alternative workplace. The employee who works at this alternative workplace is aware of the arrangement, and will make room for this key player if necessary.

In practice

An operator for mobile telephony has set up a hot site approximately 20 km from the main branch. All the GSM towers in Europe are managed from this centre and a failure of this central operational centre could result in a loss of tens of millions of Euros. The costs of this hot site are far less than the costs involved if the system were to fail for some time.

Redundant site

A good alternative for a business with many locations but only a single central computing centre is a redundant site. The redundant site contains a copy of the computing centre. All the data that enters the main computing centre is also entered into the system of the redundant site. Should one of these

two locations experience a failure, the other location will automatically take over. When this is done smoothly, the user will not notice a thing.

Hot site on demand

Another solution is a mobile hot site. This is a truck that contains all the equipment necessary to function as a temporary computing centre. The possibilities are limited, but it is one way of getting the most crucial processes operational again.

Testing the BCP

These various solutions, varying from cheap to expensive, sound very effective. A good BCP/DRP team will consider all the eventualities, discuss everything numerous times and eventually gain the approval of senior management. The plan then goes to the printer's and all managers receive a copy. But then the copies go into a cabinet or drawer. After all, disasters only happen to other people, not us. Don't they?

Well, that is why it is best to test these plans regularly, and to evaluate and modify them when necessary. Organizations change, therefore measures have to change with them.

The fact that the chance we will need the plan at all is so small is the very reason why we have to be particularly prepared. If the personnel have not been trained and the disaster becomes reality, then a BCP will not work. Regular tests are necessary to make personnel aware of how to act in the event of a disaster.

Secondly, every change that is made to the business processes must be included in the plan. An outdated plan will not help the organization to become operational again.

We can test as extensively as we like, from listening to the fire alarm to starting up a hot site or restoring a back-up. What is essential in all this testing, however, is that the procedures are tried out in a simulation of a real-life situation in order to see whether these measures are correct and effective.

These sorts of matters also have to be arranged.

A company had arranged a redundancy site. So everything appeared well organized. However, when fire broke out at the main office, it turned out that the redundancy site did not have any stores of official company letter paper. The company had to wait for the delivery of the company letter paper before work could continue. Another example is that, while a stand-by arrangement is being used, a company still has to be accessible via its standard telephone number.

Personnel measures

A disaster may result in personnel problems if the persons who support the primary process are also directly involved in the disaster and, as a consequence, are no longer available. Plans must include ways to replace these persons.

9.4 Managing communication and operating processes

9.4.1 Operating procedures and responsibilities

In order to maintain an effective management and control of the IT of an organization, it is important to document procedures for the operation of the equipment and to assign responsibilities for required activities to the appropriate people. Details can be provided through work instructions, such as how computers are turned on and off, making backups, maintenance, processing mail, etc. A PC running on Windows can be forgiving if switched off incorrectly, whereas a Unix PC tends to respond quite differently. That's why procedures for starting up after a system failure are so important.

An operating procedure includes:

- How to deal with information;
- How, when and what backups are made;
- Contact persons in the event of an incident;
- Management of audit trails and log files.

The ultimate purpose of an operating procedure is to make sure there are no misunderstandings regarding the manner in which the equipment has to be operated. This is irrespective of whether it is a welding robot, a program that controls a power station or an accounting program.

The audit trail and system log files keep a record of all the events and actions on the system and network. These files are stored in a safe place and cannot, in theory, be modified. In the event of problems, these files are often crucial in discovering what went wrong. Consider the black box in an airplane which can establish what happened in the last few minutes before a crash. On the basis of this information, measures can be taken to ensure that the incident does not happen again.

9.4.2 Change Management

The implementation of a change can lead to a catch 22 situation. Both implementing and not implementing the change involves a risk. This situation can arise, for example, in the case of a known vulnerability. Not installing a necessary patch is a risk as the vulnerability may be taken advantage of and can lead to disruptions in the infrastructure. On the other hand, installing the patch is also a risk, as unforeseen circumstances (for example due to the stability of the systems) could lead to disruptions. This example also illustrates the necessity of defining different roles in the event of changes. For instance, the potential risk of not installing a security related patch is determined by the Information Security Officer (ISO), whilst the risks associated with the change must be assessed by the manager of the system.

If changes have to be made to IT services and information systems, then these have to be carefully considered in advance and carried out in a controlled manner.

In IT Service Management, this process is called **change management.**

Change management manages changes in systems. These are often changes that have been planned in advance. An example of a small change is an alteration to a data table. A medium-sized change is, for example, changing from Microsoft Office 2000 to Microsoft Office 2003. A change has consequences that have to be known and prepared for in advance. Personnel have to learn how to work with the new version. Standard forms have to be modified, and the service desk personnel have to be trained in order to be able to continue providing support.

A large change can be a change of production system, which would therefore require more preparation and organization.

Production systems should only be changed if there are substantive reasons to do so, such as an increased risk for the system. Updating systems with the latest version of an operating system or application is not always in the interest of a company, as this can sometimes result in greater vulnerability and instability.

This example shows why a segregation of duties is so important. If everyone were able to implement their own changes, an uncontrollable situation would arise in which people would not be aware of the changes implemented by others. Even more importantly, it would quickly become impossible to identify which change was responsible for any problems that might come up and it would not be known which change may need to be reversed.

9.4.3 Segregation of duties

See also: Personnel.

Tasks and responsibilities must be segregated in order to avoid the chance of unauthorized or unintended changes or the misuse of the organization's assets (Also refer to the explanation given to the terms integrity and confidentiality).

In the segregation of duties, a review is conducted as to whether a person carries out decision-making, executive or control tasks.

It is determined whether the person needs access to information. Unnecessary access increases the risk of information being intentionally or unintentionally used, altered or destroyed. This is called the 'need to know' principle. The average employee at a company listed on the stock exchange, for example, does not have access to company information relating to its performance on the stock exchange, such as the expected profit and loss and annual figures. This prior knowledge could lead to insider trading, which is illegal.

Once personnel function and access needs are determined, tasks can be split up in order to reduce the risks for the organization. One example is the transfer of large amounts of money. One member of staff prepares the transaction and another authorizes the entry. There can be another member of staff who checks whether the transaction has been carried out correctly and legitimately.

It can be difficult for small companies to apply a segregation of duties, but this principle should be applied for as far as this is possible and practical.

9.4.4 Development, testing, acceptance and production

In order to ensure that changes cannot be implemented in an uncontrolled manner, it is also advisable to set up various (physical) environments for the development, testing, acceptance and production of information systems.

For the development phase, specific security requirements apply. The test environment is intended to determine whether the development meets the requirements and, more specifically, the security requirements.

The acceptance environment is the environment in which end users can check whether the product meets their specifications. After acceptance, a system can then be put into production following set procedures. During the transition from the existing software to the new software, there must always be a fall-back plan so that, in the event of a major problem, it is possible to revert to the old version.

In the news

A customer of the Dutch national railways (NS) discovered that anyone who knew his membership number and surname would be able to gain access to his personal data. Basically, it is possible to register on the website for a new online NS account, without it being checked whether the account already exists. Any person with malicious intent would then be able to enter in a new username, new password and new e-mail address. A link then would be sent to this new e-mail address on which the fake customer could click and thereby activate a new account. The old account would still remain active, but, through these methods, others would be able to gain access to the customer's data. They would be able to see the person's address, telephone number and any requests made for services, such as a public transport chip card, a new subscription or a change of address notification.

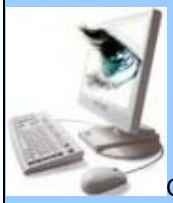
A senior security consultant dealing in access and identity management said, "The error was an elementary one and would easily have been eradicated using Tmap® (a method for standardized testing). The fact that this was not done points to a sloppy process. The chance is therefore small that this is the only error. Writing software is still not a simple process yet, and writing a correct and secure software program is highly complex. What's more, in many projects insufficient attention is given to the security. In some cases, people think that they can simply add it later. This fundamentally does not work. If you wish to secure data correctly then you have to give this the necessary attention, right from the moment that the functional specifications are set down. Security must never be approached as if it were a project. It is a quality feature of a system. You must not only test whether an application does what it is supposed to do, but also whether it does not do what it should not do."

9.4.5 Management of services by a third party

Not all activities important to an organization are carried out by the organization itself. As soon as something is to be carried out by a third party, it is important to document the requirements that the party has to meet. For example, you would not ask a handy neighbor to fill in your tax returns, but call upon the services of a tax consultant. You will assume that the tax consultant will handle your information confidentially; with a certified consultant this is required by a code of conduct.

When a company decides to outsource some or all of its IT, a good contract has to be signed with the party providing this service in which all the security aspects are given the necessary attention.

In the news

 One third of IT professionals misuse administrator passwords in order to find confidential information. A study conducted among 300 IT professionals has revealed that 33% secretly browse through the data of others, whilst 47% have on occasion looked at information that is not relevant to them.

"The only thing you need is the correct password or accounts with sufficient rights, then you can find out everything that is going on in a company," says Mark Fullbrook of Cyber-Ark.

Administrator passwords are changed less often than user passwords. Thirty percent are changed each quarter, whilst 9 percent are not changed at all. In this way, it is possible for employees who have left the organization to continue to have access to confidential information. What's more, half of the system managers do not require any authorization to gain access into accounts that have certain rights.

The study also revealed that a great deal of work still has to be done with regard to the storage of passwords. Some 57% of companies store passwords manually, 18% put them in Excel spreadsheets and 82% of the IT professionals simply try to remember them.

It is common practice to arrange a Service Level Agreement (SLA) in which both parties describe which services they expect to be carried out and under which circumstances. Audits are regularly carried out to see whether these agreements are being observed.

9.4.6 Protection against malware, phishing and spam

Malware is a combination of the word Malicious and Software and refers to undesired software such as viruses, worms, trojans and spyware. A standard measure against malware is to use antivirus scanners and a firewall. It is, however, becoming increasingly clear that a virus scanner alone is not enough to stop malware. One of the main reasons for the outbreak of viruses is human actions. A virus infection can often occur by a user opening an attachment in an e-mail that contains more than just the promised game, document or picture, but also a virus. It is therefore advisable not to open any suspicious e-mails or e-mails from unknown senders.

Phishing is a form of internet fraud. Usually the victim will receive an e-mail asking him or her to check or confirm an account with a bank or service provider, for example. Sometimes instant messaging is used. Even telephone contact has been tried. It is difficult to catch up with the perpetrators of phishing. Internet users have to remain particularly vigilant and must never respond to an e-mail request to transfer money or submit personal (financial) information, such as bank account numbers, PIN codes or credit card details.

In practice

Dear Planet Webmail subscriber,
We are currently make maintenance on your Planet.nl account. To finish this process you must give answer this message and give current username here ( ) and password here ( ) if you are the right owner of this account. Our Message Center will confirm your identity with inclusion of your secret question and answer immediately.
The new Planet.nl Webmail is a quick and light application to quick and simple access your e-mails. Also this process will help us to battle spam mails. Not give your password, makes your e-mail address inactive from our database.
You can also confirm your e-mail address by logging on your account at Planet.nl Webmail: https: / / webmail.planet.nl
PLEASE NOTE: You send a password reset message in the coming seven (7) workdays after this process for security reasons.
thank you for using Planet.nl Webmail!
https: / / webmail.planet.nl

(Editor: Please note the poor grammar!)

In the news

 An attack on Dutch tax payers was discovered that attempted to steal not only bank details, but also credit card details, tax and social insurance numbers and PIN codes. This attack, which is possibly the work of a Dutch virus designer who struck previously via MSN, consisted of two parts, whereby malware changed the homepage of the victim. That page then linked to a hacked.nl domain. (According to the cache of Google, the domain tt-ribbons.nl).

The following text appeared on the hacked page page: "At present google.nl has been referred to the tax authority services in collaboration with google.nl and your ISP. It is compulsory for you to enter the requested details. The benefit for you is that for the next few years you will no longer have to send any tax returns as this will be done automatically by the new system of the tax authorities. It is important that you have the following products handy: identity card, cash card (of the account in which your salary is deposited) and credit card. This applies only for the person in a family/relationship who has the highest income."

The victims were even threatened: "Your IP address has been stored in the database of the tax authorities," and the site showed the IP address of the visitor. In order to give this all a legitimate feel the site also featured a "Hacker Proof" certificate and a Microsoft Certified Professional logo.

In the news

Figures on the victims of identity fraud and theft are fairly sparse. One organization that wants to change this is the Dutch SAFECIN. This pilot project, which stands for the Association for Tackling Financial and Economic Crime in the Netherlands, aims to provide the first analysis in the Netherlands of normal citizens' experiences with the misuse of their identity. This project will run until 15 August and is being supported by a fraud working group using identity details from the Dutch National Platform for Crime Control.

On the Dutch website identiteitsfraude.nl, everyone who has experienced the misuse or theft of identity data can recount their own story. These include the misuse of document hard copies as well as phishing techniques through electronic means.

The researchers are particularly interested in the process in which normal citizens can become embroiled once it has become clear that they have been the victims of misuse, such as when they discover a debt at a credit institution, when they receive demands from debt collection agencies and are visited by bailiffs. Citizens who have registered and are still experiencing problems will be provided with help. The first 50 people who registered with a clear story were given a shredder as gift.

Spam is a collective name for unwanted messages. The term is normally used for undesired e-mail, but undesired advertising messages on websites are also regarded as spam. The costs of spam are passed onto the recipients: compared to the very few people who are actually interested in these messages, the great majority waste a great deal of time removing these messages from their mailbox.

A spam filter can ease the burden of this somewhat. There are a few things that computer users can do to combat spam. Some of these are to never answer a spam message—even to "opt out" or "cancel" causes more spam as you are thereby confirming for the spammer that they have a working e-mail for you and your spam will increase. Moreover, do not forward spam messages and do not distribute e-mail addresses (use the BCC functionality).

In the news

By far, the great majority of messages sent in 2007 were spam. According to CleanPort, which measures the spam percentage in the Netherlands, 96% of the e-mails were undesired advertising.

When sending messages, the spammers often responded to current events. 'In this way they hoped the recipients would be more inclined to open them,' says CleanPort. In particular, political events that made big news caused an increase in the number of spam mails.

The measurements also revealed that much spam was sent as an e-mail attachment. This helped to by-pass spam filters. However, only 0.2% of these e-mails contained viruses. This could be because virus designers in 2007 concentrated more on delivering malware via web pages instead of e-mail.

Malware, phishing and spam are important subjects in the code of conduct and security awareness campaign for employees.

In the news

Many people these days bank through the Internet. It is convenient and safe. But there is also a downside. Criminals will always try to commit fraud through the Internet.

Internet banking has experienced enormous growth in the last few years. Research carried out by the Dutch Association of Banks has shown that 98% of those who bank through the Internet regard it as safe. However, some 20% do not take enough security measures. Banks work on a daily basis to keep secure, but the responsibility for security also lies with the consumer.

This led to the '3 rights' campaign in the Netherlands:

1. Is your PC security right?
2. Is the website of your bank right?
3. Is your payment right/correct?

Attentiveness can help to avoid a great deal of damage.

9.4.6.1 Some definitions:

a) Virus

Definition:
A virus is a small computer program that purposefully replicates itself, sometimes in an altered form. The replicated versions of the original virus are, by virtue of this definition, also viruses. In order for the virus to spread it is dependent upon carriers that contain executable code.

Explanation:
As soon as the carrier is activated, the virus searches for new suitable carriers and tries to infect them. The virus can only spread outside the reach of the infected system if a user transfers files from the infected system to a new system.
Carriers were traditionally only programs, but these days documents can act as a host for a virus as they increasingly contain executable codes, such as macros, VBScript, or ActiveX. In the great majority of cases, viruses are equipped with a payload that houses all tasks other than those that are necessary for replication. This payload is usually, but not necessarily always, destructive in nature.

Examples:

Brain
Chernobyl

Measures:

- Ensure that there is a virus scanner on the mail server and on the individual computers at the workplace. Always have a virus scanner with updated definitions.
- Ensure that the subject of viruses is included in a security awareness campaign
- Ensure that this subject is included in the organization's information security policy.

- Ensure that there are effective ways of reporting incidents and that there are good follow-up procedures.

b) Worm

Definition:
A worm is a small computer program that purposefully replicates itself. The results of the replication are copies of the original spreading to other systems by making use of the network facilities of its host.

Explanation:
Although the differences between viruses and worms are becoming increasingly blurred, they still each have a number of distinctive features. A virus can attack its host via different carriers and infect new carriers by transferring active code in these new carriers. A worm in contrast does not depend on a user to spread itself: as soon as a worm is activated it can spread itself automatically. It is this that enables worms to infect large areas in a short period of time.
The two most important similarities are the dependency on an executable code in the carrier and the use of a payload in order to carry out secondary, usually destructive, tasks.

Examples:

Melissa
I love you
Happy99
Blaster
Storm Worm

Measures:

- Ensure that there is a (virus) scanner on the mail server and on the individual computers at the workplace. Always have a virus scanner with updated definitions.
- As worms can be discovered in the network, ensure that you use a network monitor tool.
- Ensure that the subject of worms is included in a security awareness campaign.
- Ensure that this subject is included in the organization's information security policy.
- Ensure that there are effective ways of reporting incidents and that there are good follow-up procedures.

c) Trojan

Definition:
A trojan is a program which, in addition to the function that it appears to perform, purposely conducts secondary activities, unnoticed by the computer user, which can harm the integrity of the infected system.

Explanation:
Just as with the real Trojan Horse, a trojan presents itself as something useful**,** but when activated by the user, it conducts all sorts of undesired activities in the background. The payload of a trojan often installs a "backdoor", through which unknown persons can gain unauthorized access to the infected system. Another frequent activity of trojans is that they send confidential information from the infected system to another location where it can be collected and analyzed.
The most noticeable difference with viruses and worms is that trojans cannot self-replicate. As a result, trojans are usually able to carry on doing their work unnoticed for a longer period of time.

Examples:

BackOrrifice

Netbus

Measures:

- Ensure that there is a trojan and/or virus scanner on the mail server and on the individual computers at the workplace. Ensure that the virus scanner is regularly updated.
- Ensure that the subject of trojans is included in a security awareness campaign; for example, staff must be aware of the dangers of opening attachments of suspicious e-mails.
- Ensure that this subject is included in the organization's information security policy.
- The consequences of trojans (communication) can also be discovered in the network by network managers; network monitor tools are available for this.
- Another measure is the use of a personal firewall at the workplace itself in order to detect suspicious network traffic.
- Ensure that there are effective ways of reporting incidents and that there are good follow-up procedures.

d) Hoax

Definition:
A hoax is a message that tries to convince the reader of its veracity and then persuades the reader to carry out a particular action. The spread of a hoax depends on readers deliberately sending the message to other potential victims who may then also do the same.

Explanation:
The payload of a hoax is not technical in nature but psychological. By playing upon people's emotions, the hoax tries to persuade the reader to send the hoax to others (a form of social engineering). This is nearly always the purpose of a hoax, but a hoax may on occasion try to convince a person to deposit money, provide personal information (phishing) or the like. Chain letters are the most significant and successful form of hoaxes.

Examples:

Good times
Pen Pal

Measures:

- Ensure that there is a virus scanner at the workplace and an antispam solution for the mail server. A hoax often contains texts that can be recognized by such scanners.
- Ensure that the subject of hoaxes is included in a security awareness campaign; staff must be wary of strange questions in e-mails, particularly those that try to convince the reader to carry out certain actions like forwarding the hoax to others.
- Ensure that this subject is included in the organization's information security policy.
- Ensure that there are effective ways of reporting incidents and that there are good follow-up procedures.

e) Logic Bomb

Definition:

A logic bomb is a piece of code that is built into a software system. This code will then carry out a function when specific conditions are met. This is not always used for malicious purposes. A computer programmer, for example, may build in a code which destroys (sensitive) files once they leave the company network. Viruses and worms often contain logic bombs, which usually have a built-in delay for the execution of the virus or the spread of the worm.

Measures:

For software written by company personnel or under contract with a third party, ensure that a code review is conducted by another party.

f) Spyware

Definition:
Spyware is a computer program that collects information on the computer user and sends this information to another party. The purpose of this is to make money. Spyware does not purposely try to damage the PC and/or the installed software, but rather to violate privacy.

Spyware can sometimes be recognized in a number of ways, for example:

- The computer is slower than usual;
- Programs are running on the computer that you have not started yourself or that you have never seen before;
- The settings on the computer have been modified and there may be a toolbar in your internet browser that was not there before and cannot be removed;
- All sorts of pop-ups appear with no prompting or when opening web pages.

Measures:

- Ensure that the software at the work place is regularly updated.
- There are scanners that scan the windows registry for suspicious registry keys and scan the installed software for spyware. Sometimes anti-virus programs can detect spyware as well.
- Use a personal firewall in order to detect suspicious network traffic, especially traffic leaving your computer with no reason.
- Ensure that the subject of spyware is included in a security awareness campaign. Staff must be wary of strange questions in e-mails, particularly those that try to convince the reader to carry out certain actions.
- Ensure that this subject is included in the organization's information security policy.
- Ensure that there are effective ways of reporting incidents and that there are good follow-up procedures.

g) Botnets / Storm Worm

Since January 2007, the Internet has been plagued by the Storm Worm, a so-called botnet, which, according to various estimations, has infected millions of computers.
Storm Worm is patient, and therefore difficult to detect and analyze. It works like a colony of ants, whereby there is no central command and control server, but rather a network connection between thousands of infected PCs is set up. As a result, the infected machines do not affect the botnet. What's more, Storm Worm does not cause any damage or load to the host, so that the hosts do not know that they are infected.

The number of e-mails with links to virtual postcards or YouTube films that attempt to spread the Storm Worm is increasingly rapidly. On 15 August 2007 there was even an actual 'pandemic' when 600,000 e-mails were sent in less than 24 hours. This allowed the Storm Worm botnet to develop into a network that is estimated now to comprise millions of infected computers all over the world.

Although the text and title of the enticing messages for the Storm Worm are constantly changing, the e-mail continues to contain a simple text or HTML code with a link to an IP address. That IP address provides a link to another infected machine within the botnet which immediately takes the user to a

server in an attempt to infect the victim with Storm Worm.
The reason that Storm Worm is such a success is that the servers that spread the Storm Worm, recode the virus message every thirty minutes, changing the signature of the virus and making it difficult to detect by traditional anti-virus programs.
So why not simply disconnect the server, you may ask? Each computer on the Internet has an IP address and can be quickly traced. That is true, but these criminals are even quicker: just like with other botnets, the location of the computers that operate the botnet are protected behind a rapidly changing form of IP addressing (for the more technically-minded: the DNS technique 'fast flow'). The consequence is that the hosting site (where the Storm Worm is lying in wait) and the mail servers (which send the enticing messages) are difficult to detect and disconnect from the network.
As a result of the recent Storm Worm activities, the number of e-mails with a link to the infected code increased massively in August 2008 to 19.5 per cent. This represented an increase of some 19 percent compared to the July figures, when 'contaminated' e-mails constituted only 0.5 per cent of all e-mails.
Further analyses of web trends have shown that the number of suspicious websites is increasing hugely on a daily basis. In August 2007 an average of 1,772 new infected websites were detected and blocked every day. This made a daily increase of 783 websites when compared to July 2007, only one month earlier.

Measures:

- Ensure that the software at the work place is regularly updated.
- There are scanners that scan the windows registry for suspicious registry keys and scan the installed software for worms. Sometimes anti-virus programs can detect worm activity as well.
- Use a personal firewall in order to detect suspicious network traffic,
- Worms can also be discovered in the network; network monitor tools are available for this.
- Ensure that the subject is included in a security awareness campaign. Staff must be wary of strange questions in e-mails, particularly those that try to convince the reader to carry out certain actions. Suspicious websites should be avoided; there is a software indicating in your internet browser when a website might be unsafe.
- Ensure that this subject is included in the organization's information security policy.
- Ensure that there are effective ways of reporting incidents and that there are good follow-up procedures.

h) Rootkit

A **rootkit** is a set of software tools that are often used by a third party (usually a hacker) after having gained access to a (computer) system. The rootkit hides itself deep in the operating system, possibly resulting in the operating system becoming unstable. A rootkit is almost impossible to remove without damaging the operating system.

Generally speaking, rootkits can work on two levels: kernel level and user level. Modern processors can handle programs in kernel mode and in user mode, and it is this difference that is fundamental: programs in kernel mode have access to the entire memory area whereas applications in user mode are limited to specific memory segments. Rootkits with kernel strategies can therefore do almost anything they want in the working memory. The purpose of these tools is to read, alter or influence the running processes, system data or files. A rootkit helps the intruder to gain access to the system, without the user noticing anything.

There are rootkits for almost every operating system. There are rootkits available for Linux, Solaris, Mac OS and most versions of Windows among others.

Rootkits became known more publically in the fall of 2005 when it came to light that the record company Sony/BMG installed rootkits through their music CDs in order to install an anti-copying security.

At the end of Augustus 2007, rootkits were introduced again to Sony products. This time it was in order to protect memory sticks. A rootkit was used in order to provide better protection, but unfortunately not enough attention was given to the further implications when applying this controversial security measure.

This security measure was actually not developed by Sony itself, but by the Taiwanese company FineArt Technology.

Rootkits are extremely difficult to detect, and infect the system often without the user noticing anything. The sole purpose of a rootkit is to create and hide files, network connections, memory addresses and index entries. Even when the rootkit has been removed, the changes that the rootkit has made to the system remain unchanged and are usually undetectable. In other words, the only way to be totally sure that a rootkit has been removed is to format and reinstall the entire system from scratch. These days (end 2006), the most modern of anti-malware software is capable of detecting and removing active rootkits as well.

The name **rootkit** comes from the UNIX environment: **root** refers to the so-called super user in UNIX. In the 1980's, hackers succeeded in infiltrating UNIX systems and installing backdoors, which allowed them to repeatedly takeover the machine with root rights.

Measures:

- Ensure that the software at the work place is regularly updated.
- There are scanners that scan the windows registry for suspicious registry keys and scan the installed software for rootkits. Sometimes anti-virus programs can detect rootkit as well, however it is recommended to use special tools that trace and destroy rootkits.
- Use a personal firewall in order to detect suspicious network traffic, rootkit software can make use of network traffic.
- Rootkits make use of the processor capacity and intern memory. Even though rootkits are well hidden, there are programs that can detect it.
- Ensure that the subject is included in a security awareness campaign. Staff must be wary of strange questions in e-mails.
- Ensure that this subject is included in the organization's information security policy.
- Ensure that there are effective ways of reporting incidents and that there are good follow-up procedures.

9.4.7 Back up and restore

The purpose of making backups, or reserve copies, is to maintain the integrity and availability of information and computing facilities.

The consequences of the loss of information depend on the age of the information that can be retrieved from backup. It is therefore important to consider the interval at which backups are made. How much time can we allow ourselves to once again generate the information that had been lost. It is important that the backup be tested regularly.

In addition to the actual making and testing of backups, it is also necessary to consider how the backups are handled. Are the backups taken from a highly secure building and then placed in an unlocked cabinet? Or are the backups placed next to the server with the original data? Do the

backups go to a third party? Is the data encrypted? For how long are the backups stored, and does this meet the statutory storage requirements?

9.4.8 Managing network security

A significant challenge in information security is that the shared network can extend beyond the boundaries of the organization.

In the news

The protection of private wireless networks in the Netherlands leaves a lot to be desired, as almost half of the networks investigated employed easily decipherable WEP encryption or no encryption at all. During a wardrive carried out by Dimension Data, a total of 884 wireless networks were scanned, and the protection of private networks was examined. As many as 18 per cent of the wireless networks were not protected at all and 28 per cent used WEP (Wired Equivalent Privacy) that could be cracked within 2 minutes. The other 54 per cent had WPA or WPA2 (WiFi-Protected Access) which is much more secure.

"Regardless of how safe you may feel your data is when you work at home on your PC, if you use a poorly protected wireless network, all the private data that you keep on your computer is at risk. Hackers can break into the wireless network and view all the information you keep on your laptop or PC. Private data such as bank account numbers, addresses and photos can therefore easily fall into the wrong hands," says a manager at Dimension Data.

Intranet - An intranet is a private network within an organization. For the user, the int*r*anet is a private version of the Int*er*net. The primary purpose of intranet is the digital sharing of information within an organization. It can also be used for teleconferences and to facilitate and stimulate the digital collaboration in groups. Via a public network, such as the Internet, it is possible for an organization, to link together the separate parts of the intranet. Special encryption and decryption methods, along with other additional security measures, ensure the reliability of this transfer. When an organization makes part of its intranet accessible for customers, partners, suppliers or other parties outside the organization, this part is called an extranet.

Extranet - An extranet is a type of computer network within an organization. The extranet is related to the intranet. The purpose of extranet is to make company information securely available to customers, partners and suppliers outside the organization. For example, a company allows customers to place orders directly on the company network via the extranet. An extranet requires protection and privacy measures such as these to be used.

- A firewall;
- Digital certificates or other methods of user authentication;
- Encryption of the information in transit;
- VPNs (Virtual Private Networks) that communicate over the Internet.

VPN - A Virtual Private Network (VPN) makes use of an already existing network, usually the Internet, in order to enable information sharing between geographically separated networks as if it were on the company's own network. The data is effectively protected—thereby ensuring its integrity, authorization and authenticity—while it is being sent. Many technical protocols have been developed to ensure the availability of this service; currently, the most well-known and widely used protocol is IPsec.

In the news

An Australian security investigator has discovered a serious security leak in a coffee machine, whereby the attacker can change the taste and the amount of water for each cup. It is also possible to cause a Denial of Coffee, so that an engineer would have to be called out to repair the machine. The seriousness of the leak has been exacerbated by the fact that the coffee machine cannot be patched. The problem arose when the machine was fitted with an Internet Connection Kit.

Through this kit, which can be installed on Windows XP, the coffee machine can communicate with the internet via the PC. This allows a user to download parameters in order to configure the espresso machine according to his or her own preference. In the event of a problem, an engineer can carry out remote diagnostic tests and provide a possible solution without the user having to leave the kitchen.

The investigator discovered that it is possible to remotely take over the XP system and software using the rights of the logged-in user. As far as we are aware, this vulnerability has not yet been exploited.

9.4.9 Handling media

Used here, “Media” refers to anything on which data can be recorded: paper, CDs, DVDs, USB sticks, hard disks, backup tapes, blackberries, mobile phones, etc.

The purpose for having guidelines for how to handle media is to avoid valuable information getting into the wrong hands and to prevent the following consequences: unauthorized publication, change, deletion or destruction of assets or an interruption of business activities.

The manner in which the media must be handled is often linked to the classification or grading, and is documented in procedures. After the storage term has expired, files with sensitive information are put into the shredder or destroyed by a certified company. USB sticks are emptied, preferable using a “wipe” tool that securely destroys the data. In addition, PCs ready for disposal are not simply thrown out with the garbage.

In practice

We always thought that a CD-Rom would last forever. In reality, however, after two to five years most of the CDs we have burned ourselves have lost so much quality that most of the data is unusable.

A number of important points:

- Media must be removed or deleted in a safe way if no longer required;
- System documentation and manuals must be kept in a secure place and updated regularly;
- The transport of media, which is of course packed well, should be carried out by a recognized courier firm that provides the correct physical conditions (humidity, temperature, electromagnetic protection).

In the news

A hospital in the state of Utah in the U.S. has lost backup tapes containing the data of at least 2.2 million patients. The data was on backup tapes and includes information about every person treated at the hospital over the last 16 years. The tapes contain diagnostic information, names, demographic information and many other sensitive items.

A hauler was to transport the tapes, but an employee decided to take the tapes home in his own car. While in his house, they were stolen, probably by a burglar who thought it was a cashbox. The employee, who had worked for the company for 18 years, was dismissed.

9.4.10 Mobile equipment

Use of mobile equipment is growing exponentially and has ever-growing capabilities. It is therefore advisable to have rules for such equipment. Just think about the implications of the loss of such devices. They are more than just hardware; they also contain software and data. Many incidents occur that involve mobile equipment. Laptops are stolen from cars every day. It is often simple to spot a laptop bag amongst other baggage at any airport, making things easier for thieves. It is difficult to obtain insurance against this type of loss. Leave your mobile equipment at work if possible, otherwise provide a suitable means of storage when travelling, combined with insurance.

Procedures for handling information

As discussed in 8.1.4 above, procedures must be developed for storing and handling information in order to protect it against unauthorized publication or misuse. The best method for this is classification or grading. This concept should be extended to mobile devices. Devices authorized to use more sensitive data should be required to use stronger measure to protect against unauthorized access or the strongest measures should be applied to all mobile devices.

Regulations must take account of the following areas:

- The position with regard to the general security policy of the organization;
- How, when, under which circumstances may classified information leave the organization;
- What classification or gradings are authorized for use;
- In addition to the grading, what designation can be used;
- For how long is the grading valid;
- Who is allowed to assign the grading;
- Under which circumstances and by whom can the grading be amended and/or terminated;
- Based on the grading, what are the confidentiality requirements;
- What security measures have to be taken in order to meet the confidentiality requirements.

In practice

A question that returns each year in the Netherlands is how long before the Queen's Speech will the budget be public? This document, containing the country's financial and economic details for the coming year, can be compared to the annual accounts of a company. If the annual accounts were to be published too early, it could lead to insider trading in the stock market, which is illegal. That's why a company will take all the necessary steps to ensure that this information is kept secret right up to the moment of publication.

9.4.11 Exchanging information

In order to prevent information ending up with parties for whom it is not intended, it is important to make internal and external agreements regarding information exchange. The purpose of the information exchange and to what the parties have agreed should be documented. It can be agreed how often information is to be shared and in what form.

It is important to prevent information from being exchanged between persons in different (possible competing) companies. Without clearly documented expectations, an employee or contractor may share sensitive information with the wrong party without realizing what detrimental effect this may have on the competitive position of their own company.

Increasing the awareness in this area is an important security measure.

Electronic messaging

Electronic messaging has risks not present in the case of communication on paper. That is why information exchanged digitally should be protected in a suitable manner.

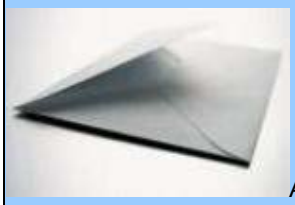
It is particularly important to be aware that when information is sent by e-mail it can be read by anyone wishing to do so. What's more, copies of the e-mail may be stored on servers spread all over the world. The Internet, after all, does not choose the shortest route, but the quickest route. The quickest route from London to Paris on a particular day may be via Moscow, New York and Berlin.

If information is highly confidential, it is best not to send it by e-mail. If there is no other way, ensure first that you protect the message through encryption.

Systems for business information

When systems within a single company are connected to one another, procedures must be developed and implemented in advance in order to protect the information against unexpected security risks.

In the news



An American internet provider accidently deleted the mail boxes of 14,000 customers. According to a spokesperson, this has never happened before and will never happen again. The spokesperson said that it is not possible to ‘undelete’ the lost data and offered her apologies.

The mistake was a result of the provider, which also provides cable and telephone services, following a practice of automatically removing inactive mail accounts every three months. In doing so on this occasion, it accidentally deleted these active accounts as well.

Although applications may be effectively protected individually, vulnerabilities can suddenly arise when they are linked. For example, in administration and bookkeeping systems where information is shared between different parts of the organization. Vulnerabilities can also arise in the connections in company communication systems, such as telephone calls or telephone conferences, confidential telephone conversations, or the digital storage of faxes.

When (highly) confidential information is involved it is important to remember that most modern office printers—which are often combined with a scanner, fax and copy function—are equipped with a hard disk. This disk stores all the information that is to be processed. Through special applications, it is often possible to gain access to that hard disk and copy all the data on it. What’s more, a ‘maintenance engineer’ could take that hard disk out of the building, often unnoticed.

In the news

An American security expert has discovered a method of sending print commands to network printers from websites. This technique could present unprecedented new possibilities for the spam industry.

Sending text to the network printer is child’s play. A potential victim only has to open the site with fraudulent JavaScript. The problem is finding out the address of the network printer, but that can be solved by running through a few IP addresses using JavaScript. By looking at the IP address of the visitor, the number of IPs to be tried can be reduced to a relatively small number.

Once found, the printer is wide open to the whims of the spammer. Not only can simple texts be printed, but also fully laid out documents, all without the user noticing anything. "It is possible to change the print settings and even send faxes," says the expert.

A hacker even gives a few tips in a document on how to make malicious use of the leak: "Create a banner page. In this way every printout has your banner page added to it. This is a handy way to distribute your message."

This is possible in both Firefox and Internet Explorer. It does not work on printers that are directly connected to the computer and not on the network.

9.4.12 Services for e-commerce

When a company decides to set up an online shop, it will start to face completely new risks than when it used the Internet only to search for information. Services for e-commerce and its use must be effectively protected. Consider, for example, secure payment transactions (Visa, MasterCard, IDeal, PayPal), the protection of the information against fraud, clear conditions in contracts, non-repudiation of purchasing and indisputable prices.

The confidentiality and integrity of order transactions, payment information including credit card details, address details of the recipient and receipt confirmation must be guaranteed and the customers have to feel confident that no strangers can gain access to all this.

Information in online transactions must be protected in order to prevent incomplete transfers, incorrect routing, unauthorized changes, unauthorized publication, unauthorized duplication or display of messages.

In the news

When a customer of an internet provider noticed that he had access to a very large file that he did not recognize, he downloaded it and found out that it contained all the customer details of an internet provider, some two-and-a-half million in total. The manager probably made an error when creating the backup file. The customer informed the service provider of this. When the internet provider did not respond, he decided to share his experiences with an internet forum.
"What happened here is wrong," said a spokeswoman from the internet provider. "Normally this sort of notification would go to our security team, who would deal with it immediately."

Conclusions:
The first error was in the backup procedure.
The second error was that the incident procedure was not followed, resulting in no response to this notification. It was only when the damage was done and the error became public that the provider responded.
Fortunately, in this case the person who made the discovery went no further than reporting this on a forum. He also could have published the entire list on the Internet, or could have sold the customer details, after which the customers concerned would have been inundated with spam or at significant risk of identity fraud.

9.4.13 Publically available information

Company information that is presented to the entire world on an internet page is public, but it still has to be correct and unable to be manipulated. Erroneous information will damage the reputation of the organization. It would be extremely annoying if you checked a company's website to find their bank details for a bill you had to pay, and then later found out that it was incorrect and that money had been deposited elsewhere.

It may be that information available on a public system—for example information on a web server that is accessible via the Internet—has to meet legislative and regulatory requirements of the jurisdiction in which the system is located, the transaction occurred or the owner resides.

It is also important that a computer program that has been made available meet the requirements of security and of the user. Consider, for example, the tax return programs of the tax authorities.

9.5 Summary

We now understand that policy gives direction to the way in which we set up information security. Policy is also used to show the government and other supervisory bodies that the legislative and regulatory requirements are being met. In addition, policy acts as an aid for employees whenever it is not clear what is or is not permitted.

We also looked at the various organizational measures. How does the organization carry out the policy? What rules do personnel have to follow?

We now know what the PDCA cycle entails. The components of the ISO/IEC 27002 standard have been outlined and, in so doing, the relationship between the various aspects of information security has become clear.

We have explained what disasters are and how we can keep the risks involved in disasters to a minimum by preparing for them.

Communication and operating processes, test procedures, in-house management or outsourcing of the IT environment have also been discussed.

We also took a closer look at malware and how we can protect ourselves against it.

The necessity of backups was examined. We looked at the security of the network and media and discussed the exchange of information and the subject of e-commerce.

9.6 Case study

A new mobile telephone provider is vigorously active in its home market. You have been hired as the Chief Information Security Officer (CISO). You are given the task of ensuring that its customers are able to arrange all their mobile telephone matters through the Internet. The focus has to be on the privacy of the customer. The customer must be able to conduct business, arrange and modify subscriptions, view the bill, etc, twenty-four hours a day.

In addition to mobile telephony, your company offers customers broadband Internet access, with a guaranteed 100% virus-free connection.

In order to show that it meets all the security requirements, your company wishes to have itself certified.

You must ensure that the management knows everything that is going on and so can respond immediately to any problems. You are also responsible for ensuring that all personnel who are hired are reliable.

There must be alternative facilities available to take over immediately in the event of a disaster.

Provide a general outline of how you are going to carry out the security for this company. Can you provide everything that the company promises in its brochures?

10. Legislation and regulations

Introduction

Much has been said in the previous chapters about how and why information security is carried out. We have taken a close look at the risk analysis and determined a threat and risk profile. On the basis of this, we have taken physical, technical and organizational measures. Some measures are optional, whereas others are required by law.

Legislation covers the areas of privacy, tax and finance and regulations for banks and companies. A company's own policy must also be observed. With internationally operating organizations, it is possible that the policy has to be adapted for country in order to observe the legislation and regulations of that nation.

In an earlier chapter, the PDCA cycle was discussed. One of the components of that cycle is both self-monitoring and monitoring carried out by an external auditor. These are components that involve monitoring the observance of internal and external legislation and regulations.

This chapter deals with the observance of legislation and regulations and the manner in which monitoring is carried out.

10.1 Observance of statutory regulations

The primarily goal of every company is to achieve its own business objectives. This means producing a certain product or providing certain services. For example, the police and special investigation bodies ensure that certain legislation and regulations are observed. Every company, however, must observe local legislation, regulations and contractual obligations. The security requirements a company must meet are strongly related to these.

Local legislation and regulations may be designed to make it easier for internationally operating companies—whose policy is somewhat more general and whose underlying policy documents have to be adapted to the legislation in force in the country in which they are based—to do business locally. Legislative requirements may differ quite a bit, particularly in the area of privacy, and therefore the manner in which one deals with information that may be private should also differ.

In order to ensure that legislative and regulatory requirements are observed, it is always important to seek legal advice from the organization's local legal advisers or from qualified attorneys.

10.2 Compliance

Compliance can also be described as tractability, obligingness, pliability, tolerance and dutifulness. What it boils down to is that an organization must observe the organization's internal regulations as well as the laws of the country and requirements of local legislation and regulations.

Sometimes this can cause conflicts. Multinational organizations in particular have to adhere, on the one hand, to its internal policy, to ensure that the company operates consistently and is seen to do so and, on the other hand, to international and local legislation and regulations.

Legislation and regulations regarding privacy are the same within the European Union, but are very different in the United States.

In practice

In Europe, privacy is well protected. In the United States, however, since the terrorist attacks on the World Trade Centre in New York, the government, out of the national interest, is allowed vast latitude on what it may do with your personal data from a security viewpoint.

On the other hand, since tens of thousands of people lost their jobs in the Enron scandal and various frauds resulted in the loss of millions of dollars, the United States employs very stringent security measures for companies quoted on the stock exchange. This legislation is the Sarbanes-Oxley Act (SOX).

Compliance not only involves observing the legislation and regulations prescribed by governments, but internal rules also play a role. In recent years, a worldwide standard for information security has been developed in the form of the Code for Information Security that was mentioned earlier. Derived from the British Standard BS 7799, an ISO standard has been developed and is now known as ISO 27002.

Various standardization bodies in the European Union and internationally have adopted this ISO standard. Thus, a far-reaching standard in security measures has been created for government and business.

10.2.1 Compliancy measures

As a result of the above, it has become clear that producing internal policy within an organization is *the* way to become compliant.

The organization must produce policy in which it declares that is must comply with the national and local legislation and regulations. Procedures and aids must be developed that make it clear to employees how to apply those regulations in practice. Risk analyses must be conducted to ensure that the right security levels are set and the appropriate measures for those security levels are determined and implemented.

10.3 Intellectual Property Rights (IPR)

When a company uses software, the use of material which could be subject to intellectual property rights must be considered.

The following guidelines need to be considered in order to protect material that may be considered intellectual property:

- Publish a policy regarding to compliance with intellectual property rights, in which legal use of computer programs and information products are defined;
- Maintain an awareness of the policy for the protection of intellectual property rights; include in the IPR policy the disciplinary measures the organization will take against any employees who violate this policy;
- Intellectual property rights include copyright to computer programs, documents, design rights, trade marks, patents and source code licenses;
- Only purchase computer programs from well-known and recognized suppliers to ensure no copyright is infringed;
- If open source is used, the associated license form must be respected and observed;

- Maintain a register of assets and identify all assets with requirements regarding the protection of intellectual property rights;
- Computer programs that are subject to property rights are usually supplied on the basis of a license agreement which states the license conditions.

In practice

It is easy, once a number of licenses of a particular computer software have been purchased, to provide new PCs with software from the same stock of licenses. Five PCs have been given a photo processing software and there are five licenses. Then two new employees join who each get their own PC onto which the photo processing software is installed as well. But no new licenses are purchased. At that point there are seven PCs that have the same photo processing software, while licenses were purchased for only five PCs.

Another form of intellectual property right infringement is the use of an image which is subject to copyright. An example of this is a fun flyer about information security that was used in the Netherlands that showed Scrooge McDuck's safe with all his security measures.

10.4 Protecting business documents

Important business documents need to be protected against loss, destruction and forgery, in accordance with statutory and regulatory requirements. The same applies, of course, to contractual obligations and business requirements.

Registrations must be categorized according to type, for example registrations into the bookkeeping system, database records, transaction log files, audit log files and operational procedures.

For every type, the storage term and the type of storage medium has to be determined, for example, paper, microfiche, magnetic or optical storage may each be appropriate for different needs. Any cryptographic keys or computer programs that are associated with the encrypted archives or digital signatures also have to be stored in order to allow registrations to be deciphered throughout the required document retention period.

It is possible for the quality of the storage media to deteriorate over time. Therefore, procedures for the storage and handling of the selected media must be implemented in accordance with the manufacturers' recommendations. For long-term storage, the use of paper and microfiche should be considered.

Where electronic storage media are chosen, procedures need to be established to avoid information becoming lost as a result of future technological changes; to guarantee that the information remains accessible (both the media and the data format must remain readable) during the entire storage period.

Governments are subject to public records legislation. This legislation deals with the creation of archives, management, destruction, transfer to the central archive, transfer between governments and access to archives.

In practice

The latest laptops and PCs no longer have a diskette drive. The 3 ½" or maybe even 5 ¼ " diskettes with data that really must not be lost, will, in the near future, be a bit tricky to read….

10.5 Protecting data and the confidentiality of personal data

The protection of data and privacy falls under personal data protection legislation and guidelines. In addition, contractual stipulations with a customer may play a part.

Every organization should have a policy for the protection of personal data and this policy should be known to everybody who processes personal data.

Observing this policy and all the relevant legislation and regulations for data protection can often best be achieved by appointing a person who is specifically responsible for the protection of data and who gives support to managers, users and service providers in the execution of their duties in this area.

Of course, there also has to be technical and organizational measures to protect personal data.

It is an important point that the citizen has the right to inspect his or her registered data. Organizations should have a policy and procedures in place for this.

In the news

In Australia, there has been quite a commotion about the government's plan to make a database containing very detailed profiles of 480,000 primary school pupils available via an intranet application. The database shows the information of all pupils in state schools and contains photos, personal information, possible career, extracurricular activities and the pupil's performance. Parents are worried not only about the privacy of their children, but also about the possibility that pedophiles will gain access to the database.

According to a professor of Informatics, this concern is justified. "People will try to get onto the database; I do not doubt that for a minute." Pupils who do not provide the obligatory information, may be refused access to the school, said the Ministry of Education who told parents they need not worry about hacking pedophiles. "We have not made a Facebook." The minister did not comment on the infringement of privacy, which goes much further than many social network sites.

The completion of the first phase of the database and its accessibility is planned for December. It will contain reports, contact details, information regarding attendance, the pupil's behavior, what he or she would like to become and the parent's contact information.

Source: www.security.nl

10.6 Preventing abuse of IT facilities

One of the aspects that management must include in the information security policy is the manner in which the IT facilities may be used within the organization. Use of these facilities for non-business purposes—or any unauthorized purpose—without the permission of management should be regarded as improper use of the facilities.

If any unauthorized activity is observed through monitoring or otherwise, this activity needs to be brought to the attention of the manager in question in order to consider whether disciplinary and/or legal measures are to be taken.

There are, of course, two sides to such matters. On the one hand, the organization needs to fully meet the regulations mentioned above with regard to the correct use of licenses; only use legal

software and observe the rules surrounding intellectual property. On the other hand, staff are expected not to abuse the IT facilities made available to them.

In many organizations, there is now a code of conduct stipulating the rights and duties of the employer and of the employees in this area.

It is, for example, often permitted to use the telephone and internet for private ends as long as the work does not suffer as a consequence. Downloading music, films and software and visiting sexually oriented sites are usually explicitly prohibited. The use of e-mail should also be subject to conditions.

The employer has the right to monitor the use to which their systems are put. This may be done in the form of random checks or in a highly targeted manner when there is a strong suspicion of misuse by certain persons. This might be on condition, however, that the employees are aware of the fact that these monitoring measures may be carried out. Conditions regarding such monitoring depend on the local legislation.

Prior to implementing such monitoring systems, it is important to gain legal advice and to consult the organization's council.

There is also legislation aimed at crimes conducted using computers. Intentionally gaining unauthorized access into a computer system is punishable by law, even if the system does not have any security. In recent years, computer criminality legislation has been tightened to counter attempts at making computer systems unusable through, for example, denial of service attacks. A denial of service is a method whereby an information system, for example a website, is inundated with requests until it can no longer cope with them and eventually fails. Botnets, networks of computers linked to one another, are often used for this sort of attack.

In the news

An 18 year-old high school student who hacked into the school's system and changed his test scores may be sentenced to 38 years in jail. Using his teacher's password, he managed to log on to the grade system and change the result of, among other things, a test which he had failed due to cheating. According to the prosecuting attorney, the student had also broken into the school and changed the grades of 12 other students. He also installed spyware on the school computers to allow him to access them from remote locations.

During the break-ins, he also changed the results forms. He changed, for example, grades and dates, so that the grades on paper matched those in the system. The case came to light when he asked for a copy of his student records to appeal against a decision of the University of California, where his application was rejected on account of his poor grades. Teachers discovered the discrepancies in the grades and alerted the police, after which an investigation was conducted.

The student has been charged with stealing public records, computer fraud, burglary, identity theft, receiving stolen property and conspiracy. Another student who conspired with him faces three years in jail. The school will take measures to avoid this happening again in the future.

10.7 Observing security policy and security standards

Information security involves responsibility at different levels. The management board will always bear the final responsibility. It can, however, assign the responsibility for the execution and observance of the policy to the line managers. Managers therefore regularly need to assess (or have assessed) whether the data processing within their area of responsibility meets the applicable security policy, security standards and other security requirements.

10.8 Monitoring measures

Finally, the internal and/or external auditor will check whether the organization complies with the regulations. The auditor does this by looking at whether such a measure is in place. Is it included in the policy? Is it observed in practice? Does the measure function as it should?

In practice

An organization has implemented the ISO/IEC 27002 standard. One of the security measures is a password policy. The policy stipulates that, in order to gain access to the office computer system, a password of 8 characters has to be used. The password must not be a known word. What's more, it should contain at least 1 capital letter and 1 number or punctuation character.

The auditor looks at the set-up: Yes, it is in the policy.

The auditor looks at whether it has been implemented: Yes, the system manager has implemented the required rules.

The auditor looks how it works in practice: He personally enters various passwords that do not meet the requirements. If the password is accepted then this security measure does not work correctly. If a password can only be entered if it meets the policy's requirements, then the measure works correctly.

10.9 Information system audits

Carrying out audits always involves risks for an organization's production process. Auditors often take information from the systems when the production process is running. This always affects the computers' processing capacity because these now have to carry out extra tasks. It is therefore important to ensure that the audit does not cause a disruption.

Due to this, it is not advisable to have a third party or a customer examine the same things. The auditor can issue a Third Party Notification to this end. This statement, issued by an independent IT auditor, indicates to what extent the necessary measures have functioned in terms of set-up, implementation and operation.

10.10 Protecting aids used for auditing information systems

The aids used for system audits, for example computer programs or databases, must be kept separate from development systems and production systems and should not be stored in tape libraries or users' rooms, unless additional protective measures of a suitable level have been taken.

If third parties are involved in an audit, there is the risk that the audit aids and the information to which this third party has access may be misused.

Measures such as limiting access to only those systems that the auditor needs for his investigation, a Non-Disclosure Agreement and limiting physical access may be considered to help mitigate this risk. Once an audit is complete, the organization should immediately change any passwords that were given to the auditors.

Finally, after everything that has been discussed, one unchangeable rule will always apply: No matter how well an organization has planned its security, security is only as strong as the weakest link!

10.11 Summary

In this chapter we have discussed the role of legislation and regulations.

There is legislation for tax matters, for privacy and for how business is conducted. There is local legislation, international legislation and regulations such as the Sarbanes-Oxley Act which stipulates that a foreign bank can only trade on Wall Street if it can show that it observes the American legislation and regulations.

We have seen that standards such as the ISO/IEC 27002 help in observing the legislation and regulations.

Intellectual property rights of others must be protected just as does the property of the organization. If a company has invested hundreds of thousands, maybe even millions in the development of a product, it naturally does not want anyone to copy it without permission and to offer it at a lower price.

Finally, an audit can demonstrate that the requirements for the security of the information are being met.

10.12 Case study

Incasso BV is a large debt-collection agency that sees to the collection of late payments for a large number of customers. Incasso BV started as a sole trader and has developed through the years into a company with five offices in the Benelux countries (Belgium, the Netherlands and Luxembourg) that also offers banking services, albeit on a small scale. The company has sixty employees.

In connection with extensive legislation and regulations, you are hired to ensure that information security is implemented in accordance with the ISO/IEC 27002 standard. You will investigate what legislation and regulations apply and, based on this information, will produce the policy.

To prove the efficacy of your program, you must commission an external audit to demonstrate that your program being properly followed.

An external audit will be conducted and you will be required to prove the efficacy of your program.

Describe what you have to do to develop the security plan. Outline which security measures have to be carried out. How will you show the auditors that your company has arranged everything properly? What legislation and regulations prescribed by the government must you deal with?

Index

sample exam

ISFS.EN_1.1

Information Security Foundation based on ISO/IEC 27002
edition April 2009

content

EXIN International B.V.
Examination Institute for Information Science
Janssoenborch, Hoog Catharijne
Godebaldkwartier 365, 3511 DT Utrecht
P.O. Box 19147, 3501 DC Utrecht
The Netherlands
Telephone +31 30 234 48 25
Fax +31 30 231 59 86
E-mail info@exin.nl
Internet www.exin-exams.com

Introduction

This is the sample exam Information Security Foundation based on ISO/IEC 27002.

This sample exam consists of 40 multiple-choice questions. Each multiple-choice question has a number of possible answers, of which only one is the correct answer.

The maximum number of points that can be obtained for this exam is 40. Each correct answer is worth one point. If you obtain 26 points or more you will pass.

The time allowed for this exam is 60 minutes.

No rights may be derived from this information.

Good luck!

Sample exam

1 of 40

You have received a draft of your tax return from the accountant and you check whether the data is correct.

Which characteristic of reliability of information are you checking?

A. availability
B. exclusivity
C. integrity
D. confidentiality

2 of 40

In order to take out a fire insurance policy, an administration office must determine the value of the data that it manages.

Which factor is **not** important for determining the value of data for an organization?

A. The content of data.
B. The degree to which missing, incomplete or incorrect data can be recovered.
C. The indispensability of data for the business processes.
D. The importance of the business processes that make use of the data.

3 of 40

Our access to information is becoming increasingly easy. Still, information has to be reliable in order to be usable.

What is **not** a reliability aspect of information?

A. availability
B. integrity
C. quantity
D. confidentiality

4 of 40

"Completeness" is part of which aspect of reliability of information?

A. availability
B. exclusivity
C. integrity
D. confidentiality

5 of 40

An administration office is going to determine the dangers to which it is exposed.

What do we call a possible event that can have a disruptive effect on the reliability of information?

A. dependency
B. threat
C. vulnerability
D. risk

6 of 40

What is the purpose of risk management?

A. To determine the probability that a certain risk will occur.
B. To determine the damage caused by possible security incidents.
C. To outline the threats to which IT resources are exposed.
D. To use measures to reduce risks to an acceptable level.

7 of 40

Which statement about risk analysis is correct?

1. Risks that are stated in a risk analysis can be classified.
2. In a risk analysis all details have to be considered.
3. A risk analysis limits itself to availability.
4. A risk analysis is simple to carry out by completing a short standard questionnaire with standard questions.

A. 1
B. 2
C. 3
D. 4

8 of 40

Which of the examples given below can be classified as fraud?

1. Infecting a computer with a virus.
2. Carrying out an unauthorized transaction.
3. Tapping communication lines and networks.
4. Using the work internet for private ends.

A. 1
B. 2
C. 3
D. 4

9 of 40

A possible risk for a company is fire damage. If this threat occurs, that is to say that a fire actually breaks out, direct and indirect damage may result.

What is an example of direct damage?

A. a database is destroyed
B. image loss
C. loss of client trust
D. statutory obligations can no longer be met

10 of 40

In order to reduce risks, a company decides to opt for a strategy of a mix of measures. One of the measures is that a stand-by arrangement is organized for the company.

To which category of measures does a stand-by arrangement belong?

A. corrective measures
B. detective measures
C. preventive measures
D. repressive measures

11 of 40

What is an example of a human threat?

A. A USB-stick passes on a virus to the network.
B. Too much dust in the server room.
C. A leak causes a failure of electricity supply.

12 of 40

What is an example of a human threat?

A. a lightning strike
B. fire
C. phishing

13 of 40

Information has a number of reliability aspects.
Reliability is constantly being threatened. Examples of threats are: a cable becomes loose, someone alters information by accident, data is used privately or is falsified.

Which of these examples is a threat to confidentiality?

A. a loose cable
B. accidental deletion of data
C. private use of data
D. falsifying data

14 of 40

A member of staff denies sending a particular message.

Which reliability aspect of information is in danger here?

A. availability
B. correctness
C. integrity
D. confidentiality

15 of 40

In the incident cycle there are four successive steps.

What is the order of these steps?

A. Threat, Damage, Incident, Recovery
B. Threat, Incident, Damage, Recovery
C. Incident, Threat, Damage, Recovery
D. Incident, Recovery, Damage, Threat

16 of 40

A fire breaks out in a branch office of a health insurance company. The personnel are transferred to neighboring branches to continue their work.

Where in the incident lifecycle are such stand-by arrangements found?

A. between threat and incident
B. between recovery and threat
C. between damage and recovery
D. between incident and damage

17 of 40

How is the purpose of information security policy best described?

A. Policy documents the analysis of risks and the search for countermeasures.
B. Policy provides direction and support to the management regarding information security.
C. Policy makes the security plan concrete by providing it with the necessary details.
D. Policy provides insight into threats and the possible consequences.

18 of 40

The code of conduct for e-business is based on a number of principles.

Which of the following principles do **not** belong?

A. reliability
B. registration
C. confidentiality and privacy

19 of 40

A worker from insurance company Euregio discovers that the expiration date of a policy has been changed without her knowledge. She is the only person authorized to do this. She reports this security incident to the Helpdesk. The Helpdesk worker records the following information regarding this incident:

- date and time
- description of the incident
- possible consequences of the incident

What important information about the incident is missing here?

A. the name of the person reporting the incident
B. the name of the software package
C. the PC number
D. a list of people who were informed about the incident

20 of 40

A company experiences the following incidents:
1. A smoke alarm does not work.
2. The network is hacked into.
3. Someone pretends to be a member of staff.
4. A file on the computer cannot be converted into a PDF file.

Which of these incidents is **not** a security incident?

A. 1
B. 2
C. 3
D. 4

21 of 40

Security measures can be grouped in various ways.

Which of the following is correct?

A. physical, logical, preventive
B. logical, repressive, preventive
C. organizational, preventive, corrective, physical
D. preventive, detective, repressive, corrective

22 of 40

A smoke alarm is placed in a computer room.

Under which category of security measures does this fall?

A. corrective
B. detective
C. organizational
D. preventive

23 of 40

The Information Security Officer (ISO) of insurance company Euregio wishes to have a list of security measures put together.

What does she first have to do before security measures can be selected?

A. Set up monitoring.
B. Carry out an evaluation.
C. Formulate information security policy.
D. Carry out a risk analysis.

24 of 40

What is the purpose of classifying information?

A. To determine what types of information may require different levels of protection.
B. To allocate information to an owner.
C. To reduce the risks of human error.
D. To prevent unauthorized access to information.

25 of 40

Strong authentication is needed to access highly protected areas. In case of strong authentication the identity of a person is verified by using three factors.

Which factor is verified when we must enter a personal identification number (PIN)?

A. something you are
B. something you have
C. something you know

26 of 40

Access to the computer room is closed off using a pass reader. Only the System Management department has a pass.

What type of security measure is this?

A. a corrective security measure
B. a physical security measure
C. a logical security measure
D. a repressive security measure

27 of 40

Four (4) staff members of the IT department share one (1) pass for the computer room.

What risk does this lead to?

A. If the power fails, the computers go off.
B. If fire breaks out the fire extinguishers can not be used.
C. If something disappears from the computer room it will not be clear who is responsible.
D. Unauthorized persons may gain access to the computer room without being seen.

28 of 40

In the reception hall of an administration office, there is a printer which all staff can use in case of emergency. The arrangement is that the printouts are to be collected immediately so that they cannot be taken away by a visitor.

What other risk for the company information does this situation have?

A. Files can remain in the memory of the printer.
B. Visitors would be able to copy and print out confidential information from the network.
C. The printer can become defective through excessive use, so that it is no longer available for use.

29 of 40

Which of the following security measures is a technical measure?

1. Allocating information to an owner
2. Encryption of files
3. Creating a policy defining what is and is not allowed in e-mail
4. Storing system management passwords in a safe

A. 1
B. 2
C. 3
D. 4

30 of 40

The backups of the central server are kept locked in the same enclosed room as the server.

What risk does the organization face?

A. If the server crashes, it will take a long time before the server is again operational.
B. In the event of fire it is impossible to get the system back to its former state.
C. No one is responsible for the backups.
D. Unauthorized persons have easy access to the backups.

31 of 40

Which of the below technologies is malicious?

A. encryption
B. hash
C. Virtual Private Network (VPN)
D. viruses, worms and spyware

32 of 40

Which measure does **not** help against malicious software?

A. an active patch policy
B. an anti-spyware program
C. a spam filter
D. a password

33 of 40

What is an example of an organizational measure?

A. backup of data
B. encryption
C. segregation of duties
D. keeping network equipment and junction boxes in a locked room

34 of 40

Identification is establishing whether someone's identity is correct.

Is this statement correct?

A. yes
B. no

35 of 40

Why is it necessary to keep a disaster recovery plan up to date and to test it regularly?

A. In order always to have access to recent backups that are located outside the office.
B. In order to be able to cope with daily occurring faults.
C. Because otherwise, in the event of a far-reaching disruption, the measures taken and the incident procedures planned may not be adequate or may be outdated.
D. Because this is required by the Personal Data Protection Act.

36 of 40

What is authorization?

A. The determination of a person's identity.
B. The registration of actions carried out.
C. The verification of a person's identity.
D. The granting of specific rights, such as selective access to a person.

37 of 40

Which important statutory norm in the area of information security does the government have to meet?

A. Dependency & Vulnerability analysis
B. ISO/IEC 20000
C. ISO/IEC 27002
D. national information security legislation or regulations

38 of 40

On the basis of which legislation can someone request to inspect the data that has been registered about him or her?

A. The Public Records Act
B. The Personal Data Protection Act
C. The Computer Criminality Act
D. The Government Information (Public Access) Act

39 of 40

The Code for Information Security (ISO/IEC 27002) is a description of a risk analysis method.

Is this statement correct?

A. yes
B. no

40 of 40

The Code for Information Security (ISO/IEC 27002) only applies to large companies.

Is this statement correct?

A. yes
B. no

Answer Key

1 of 40

You have received a draft of your tax return from the accountant and you check whether the data is correct.

Which characteristic of reliability of information are you checking?

A. availability
B. exclusivity
C. integrity
D. confidentiality

A. Incorrect. Availability is the degree to which information is available for the users at the required times.
B. Incorrect. Exclusivity is a characteristic of confidentiality.
C. Correct. This concerns integrity. See section 4.5 of "*The basics of information security*".
D. Incorrect. This concerns the degree to which the access to information is restricted to only those who are authorized.

2 of 40

In order to take out a fire insurance policy, an administration office must determine the value of the data that it manages.

Which factor is **not** important for determining the value of data for an organization?

A. The content of data.
B. The degree to which missing, incomplete or incorrect data can be recovered.
C. The indispensability of data for the business processes.
D. The importance of the business processes that make use of the data.

A. Correct. The content of data does not determine its value. See section 4.3 of "*The basics of information security*".
B. Incorrect. Missing, incomplete or incorrect data that can be easily recovered is less valuable than data that is difficult or impossible to recover.
C. Incorrect. The indispensability of data for business processes in part determines the value.
D. Incorrect. Data critical to important business processes is therefore valuable.

3 of 40

Our access to information is becoming increasingly easy. Still, information has to be reliable in order to be usable.

What is **not** a reliability aspect of information?

A. availability
B. integrity
C. quantity
D. confidentiality

A. Incorrect. Availability is a reliability aspect of information.
B. Incorrect. Integrity is a reliability aspect of information.
C. Correct. Quantity is not a reliability aspect of information. See section 4.5 of "*The basics of information security*".
D. Incorrect. Confidentiality is a reliability aspect of information.

4 of 40

"Completeness" is part of which aspect of reliability of information?

A. availability
B. exclusivity
C. integrity
D. confidentiality

A. Incorrect. Information can be available without having to be complete.
B. Incorrect. Exclusivity is a characteristic of confidentiality.
C. Correct. Completeness is part of the integrity aspect. See section 4.5 of "*The basics of information security*".
D. Incorrect. Confidential information does not have to be complete.

5 of 40

An administration office is going to determine the dangers to which it is exposed.

What do we call a possible event that can have a disruptive effect on the reliability of information?

A. dependency
B. threat
C. vulnerability
D. risk

A. Incorrect. A dependency is not an event.
B. Correct. A threat is a possible event that can have a disruptive effect on the reliability of information. See section 5 of "*The basics of information security*".
C. Incorrect. Vulnerability is the degree to which an object is susceptible to a threat.
D. Incorrect. A risk is the average expected damage over a period of time as a result of one or more threats leading to disruption(s).

6 of 40

What is the purpose of risk management?

A. To determine the probability that a certain risk will occur.
B. To determine the damage caused by possible security incidents.
C. To outline the threats to which IT resources are exposed.
D. To use measures to reduce risks to an acceptable level.

A. Incorrect. This is part of risk analysis.
B. Incorrect. This is part of risk analysis.
C. Incorrect. This is part of risk analysis.
D. Correct. The purpose of risk management is to reduce risks to an acceptable level. See section 5 of "*The basics of information security*".

7 of 40

Which statement about risk analysis is correct?

1. Risks that are stated in a risk analysis can be classified.
2. In a risk analysis all details have to be considered.
3. A risk analysis limits itself to availability.
4. A risk analysis is simple to carry out by completing a short standard questionnaire with standard questions.

A. 1
B. 2
C. 3
D. 4

A. Correct. Not all risks are equal. As a rule the largest risks are tackled first. See section 5 of "*The basics of information security*".
B. Incorrect. It is impossible in a risk analysis to examine every detail.
C. Incorrect. A risk analysis considers all reliability aspects, including integrity and confidentiality along with availability.
D. Incorrect. In a risk analysis questions are seldom applicable to every situation.

8 of 40

Which of the examples given below can be classified as fraud?

1. Infecting a computer with a virus.
2. Carrying out an unauthorized transaction.
3. Tapping communication lines and networks.
4. Using the work internet for private ends.

A. 1
B. 2
C. 3
D. 4

A. Incorrect. A virus infection is classified as the threat "unauthorized change".
B. Correct. An unauthorized transaction is classified as "fraud". See section 10.6 of "*The basics of information security*".
C. Incorrect. Tapping is classified as the threat "disclosure".
D. Incorrect. Private use is classified as the threat "misuse".

9 of 40

A possible risk for a company is fire damage. If this threat occurs, that is to say that a fire actually breaks out, direct and indirect damage may result.

What is an example of direct damage?

A. a database is destroyed
B. image loss
C. loss of client trust
D. statutory obligations can no longer be met

A. Correct. A destroyed database is an example of direct damage. See section 5.5 of "*The basics of information security*".
B. Incorrect. Image loss is indirect damage.
C. Incorrect. Loss of client trust is indirect damage.
D. Incorrect. Being unable to meet statutory obligations is indirect damage.

10 of 40

In order to reduce risks, a company decides to opt for a strategy of a mix of measures. One of the measures is that a stand-by arrangement is organized for the company.

To which category of measures does a stand-by arrangement belong?

A. corrective measures
B. detective measures
C. preventive measures
D. repressive measures

A. Incorrect. Corrective measures focus on recovery after damage.
B. Incorrect. Detective measures only give a signal after detection.
C. Incorrect. Preventive measures are intended to avoid incidents.
D. Correct. Repressive measures, such as a stand-by arrangement, minimize the damage. See section 5.3.4 of "*The basics of information security*".

11 of 40

What is an example of a human threat?

A. A USB-stick passes on a virus to the network.
B. Too much dust in the server room.
C. A leak causes a failure of electricity supply.

A. Correct. A USB-stick is always inserted by a person. Thus, if by doing so a virus enters the network, then it is a human threat. See section 5.4.1 of "*The basics of information security*".
B. Incorrect. Dust is not a human threat.
C. Incorrect. A leak is not a human threat.

12 of 40

What is an example of a human threat?

A. a lightning strike
B. fire
C. phishing

A. Incorrect. A lightning strike is an example of a non-human threat.
B. Incorrect. Fire is an example of a non-human threat.
C. Correct. Phishing (luring users to false websites) is one form of a human threat. See section 5.4.1 and 9.4.6 of "*The basics of information security*".

13 of 40

Information has a number of reliability aspects.
Reliability is constantly being threatened. Examples of threats are: a cable becomes loose, someone alters information by accident, data is used privately or is falsified.

Which of these examples is a threat to confidentiality?

A. a loose cable
B. accidental deletion of data
C. private use of data
D. falsifying data

A. Incorrect. A loose cable is a threat to the availability of information.
B. Incorrect. The unintended alteration of data is a threat to its integrity.
C. Correct. The use of data for private ends is a form of misuse and is a threat to confidentiality. See section 4.5 of "*The basics of information security*".
D. Incorrect. The falsification of data is a threat to its integrity.

14 of 40

A member of staff denies sending a particular message.

Which reliability aspect of information is in danger here?

A. availability
B. correctness
C. integrity
D. confidentiality

A. Incorrect. Overloading the infrastructure is an example of a threat to availability.
B. Incorrect. Correctness is not a reliability aspect. It is a characteristic of integrity.
C. Correct. The denial of sending a message has to do with nonrepudiation, a threat to integrity. See section 4.5 of "*The basics of information security*".
D. Incorrect. Misuse and/or disclosure of data are threats to confidentiality.

15 of 40

In the incident cycle there are four successive steps.

What is the order of these steps?

A. Threat, Damage, Incident, Recovery
B. Threat, Incident, Damage, Recovery
C. Incident, Threat, Damage, Recovery
D. Incident, Recovery, Damage, Threat

A. Incorrect. The damage follows after the incident.
B. Correct. The order of steps in the incident cycle are: Threat, Incident, Damage, Recovery. See section 6.4.4 of "*The basics of information security*".
C. Incorrect. The incident follows the threat.
D. Incorrect. Recovery is the last step.

16 of 40

A fire breaks out in a branch office of a health insurance company. The personnel are transferred to neighboring branches to continue their work.

Where in the incident lifecycle are such stand-by arrangements found?

A. between threat and incident
B. between recovery and threat
C. between damage and recovery
D. between incident and damage

A. Incorrect. Carrying out a stand-by arrangement without there first being an incident is very expensive.
B. Incorrect. Recovery takes place after putting stand-by arrangement into operation.
C. Incorrect. Damage and recovery are actually limited by the stand-by arrangement.
D. Correct. A stand-by arrangement is a repressive measure that is initiated in order to limit the damage. See section 6.4.4 and 9.3 of "*The basics of information security*".

17 of 40

How is the purpose of information security policy best described?

A. Policy documents the analysis of risks and the search for countermeasures.
B. Policy provides direction and support to the management regarding information security.
C. Policy makes the security plan concrete by providing it with the necessary details.
D. Policy provides insight into threats and the possible consequences.

A. Incorrect. This is the purpose of risk analysis and risk management.
B. Correct. The security policy provides direction and support to the management regarding information security. See section 9.1 of "*The basics of information security*".
C. Incorrect. The security plan makes the information security policy concrete. The plan includes which measures have been chosen, who is responsible for what, the guidelines for the implementation of measures, etc.
D. Incorrect. This is the purpose of a threat analysis.

18 of 40

The code of conduct for e-business is based on a number of principles.

Which of the following principles do **not** belong?

A. reliability
B. registration
C. confidentiality and privacy

A. Incorrect. Reliability forms one of the bases of the code of conduct.
B. Correct. The code of conduct is based on the principles of reliability, transparency, confidentiality and privacy. Registration does not belong here. See section 9.4.12 of "*The basics of information security*".
C. Incorrect. The code of conduct is based on confidentiality and privacy among other things.

19 of 40

A worker from insurance company Euregio discovers that the expiration date of a policy has been changed without her knowledge. She is the only person authorized to do this. She reports this security incident to the Helpdesk. The Helpdesk worker records the following information regarding this incident:

- date and time
- description of the incident
- possible consequences of the incident

What important information about the incident is missing here?

A. the name of the person reporting the incident
B. the name of the software package
C. the PC number
D. a list of people who were informed about the incident

A. Correct. When reporting an incident, the name of the reporter must be recorded at a minimum. See section 6.4.1 of "*The basics of information security*".
B. Incorrect. This is additional information that may be added later.
C. Incorrect. This is additional information that may be added later.
D. Incorrect. This is additional information that may be added later.

20 of 40

A company experiences the following incidents:
1. A smoke alarm does not work.
2. The network is hacked into.
3. Someone pretends to be a member of staff.
4. A file on the computer cannot be converted into a PDF file.

Which of these incidents is **not** a security incident?

A. 1
B. 2
C. 3
D. 4

A. Incorrect. A defective smoke alarm is an incident that can threaten the availability of data.
B. Incorrect. Hacking is an incident that can threaten the availability, integrity and confidentiality of data.
C. Incorrect. Misuse of identity is an incident that can threaten the aspect availability, integrity and confidentiality of data.
D. Correct. A security incident is an incident that threatens the confidentiality, reliability or availability of data. This is not a threat to the availability, integrity and confidentiality of data. See section 6.4 of "*The basics of information security*".

21 of 40

Security measures can be grouped in various ways.

Which of the following is correct?

A. physical, logical, preventive
B. logical, repressive, preventive
C. organizational, preventive, corrective, physical
D. preventive, detective, repressive, corrective

A. Incorrect. Organizational/logical/physical is one appropriate group, as is preventive/detective/repressive/corrective.
B. Incorrect. Organizational/logical/physical is one appropriate group, as is preventive/detective/repressive/corrective.
C. Incorrect. Organizational/logical/physical is one appropriate group, as is preventive/detective/repressive/corrective.
D. Correct. Preventive/detective/repressive/corrective is one appropriate group, as is organizational/logical/physical. See section 5.3 of "*The basics of information security*".

22 of 40

A smoke alarm is placed in a computer room.

Under which category of security measures does this fall?

A. corrective
B. detective
C. organizational
D. preventive

A. Incorrect. A smoke alarm detects and then sends an alarm, but does not take any corrective action.
B. Correct. A smoke alarm only has a signalling function; after the alarm is given, action is still required. See section 5.3 of "*The basics of information security*".
C. Incorrect. Only the measures that follow a smoke alarm signal are organizational; the placing of a smoke alarm is not organizational.
D. Incorrect. A smoke alarm does not prevent fire and is therefore not a preventive measure.

23 of 40

The Information Security Officer (ISO) of insurance company Euregio wishes to have a list of security measures put together.

What does she first have to do before security measures can be selected?

A. Set up monitoring.
B. Carry out an evaluation.
C. Formulate information security policy.
D. Carry out a risk analysis.

A. Incorrect. Monitoring is a possible measure.
B. Incorrect. Evaluation happens after the list of measures is assembled.
C. Incorrect. An information security policy is important, but is not necessary in order to select measures.
D. Correct. Before security measures can be selected, Euregio must know their risks to determine which risks require a security measure. See section 5 of "*The basics of information security*".

24 of 40

What is the purpose of classifying information?

A. To determine what types of information may require different levels of protection.
B. To allocate information to an owner.
C. To reduce the risks of human error.
D. To prevent unauthorized access to information.

A. Correct. The purpose of classifying information is to maintain an adequate protection. See section 6.3 of "*The basics of information security*".
B. Incorrect. Allocating information to an owner is the means of classification and not the purpose.
C. Incorrect. Reducing the risks of human error is part of the security requirements of the staff.
D. Incorrect. Preventing unauthorized access to information is part of access security.

25 of 40

Strong authentication is needed to access highly protected areas. In case of strong authentication the identity of a person is verified by using three factors.

Which factor is verified when we must enter a personal identification number (PIN)?

A. something you are
B. something you have
C. something you know

A. Incorrect. A PIN code is not an example of something that you are.
B. Incorrect. A PIN code is not something that you have.
C. Correct. A PIN code is something that you know. See section 7.2.2.1 of "*The basics of information security*".

26 of 40

Access to the computer room is closed off using a pass reader. Only the System Management department has a pass.

What type of security measure is this?

A. a corrective security measure
B. a physical security measure
C. a logical security measure
D. a repressive security measure

A. Incorrect. A corrective security measure is a recovery measure.
B. Correct. This is a physical security measure. See section 7 of "*The basics of information security*".
C. Incorrect. A logical security measure controls the access to software and information, not the physical access to rooms.
D. Incorrect. A repressive security measure is intended to minimize the consequences of a disruption.

27 of 40

Four (4) staff members of the IT department share one (1) pass for the computer room.

What risk does this lead to?

A. If the power fails, the computers go off.
B. If fire breaks out the fire extinguishers can not be used.
C. If something disappears from the computer room it will not be clear who is responsible.
D. Unauthorized persons may gain access to the computer room without being seen.

A. Incorrect. Computers going off as a result of a power failure has nothing to do with access management.
B. Incorrect. Even with one pass, the IT staff can put out a fire with a fire extinguisher.
C. Correct. Though it would be clear that someone from the IT department had been inside, it would not be certain who. See section 7.2 of "*The basics of information security*".
D. Incorrect. No one has access to the computer room without a pass.

28 of 40

In the reception hall of an administration office, there is a printer which all staff can use in case of emergency. The arrangement is that the printouts are to be collected immediately so that they cannot be taken away by a visitor.

What other risk for the company information does this situation have?

A. Files can remain in the memory of the printer.
B. Visitors would be able to copy and print out confidential information from the network.
C. The printer can become defective through excessive use, so that it is no longer available for use.

A. Correct. If files remain in the memory they can be printed off and taken away by any passerby. See section 9.4.11 of "*The basics of information security*".
B. Incorrect. It is not possible to use a printer to copy information from the network.
C. Incorrect. The unavailability of a printer does not form a risk for company information.

29 of 40

Which of the following security measures is a technical measure?

1. Allocating information to an owner
2. Encryption of files
3. Creating a policy defining what is and is not allowed in e-mail
4. Storing system management passwords in a safe

A. 1
B. 2
C. 3
D. 4

A. Incorrect. Allocating information to an owner is classification, which is an organizational measure.
B. Correct. This is a technical measure which prevents unauthorized persons from reading the information. See section 8.3 of "*The basics of information security*".
C. Incorrect. This is an organizational measure, a code of conduct that is written in the employment contract.
D. Incorrect. This is an organizational measure.

30 of 40

The backups of the central server are kept locked in the same enclosed room as the server.

What risk does the organization face?

A. If the server crashes, it will take a long time before the server is again operational.
B. In the event of fire it is impossible to get the system back to its former state.
C. No one is responsible for the backups.
D. Unauthorized persons have easy access to the backups.

A. Incorrect. On the contrary, this would help to make the system operational more quickly.
B. Correct. The chance that the backups may also be destroyed in a fire is very great. See section 9.4.7 of "*The basics of information security*".
C. Incorrect. The responsibility has nothing to do with the storage location.
D. Incorrect. The computer room is locked.

31 of 40

Which of the below technologies is malicious?

A. encryption
B. hash
C. Virtual Private Network (VPN)
D. viruses, worms and spyware

A. Incorrect. Encryption is making information unreadable to anyone except those possessing special knowledge, usually referred to as a key.
B. Incorrect. Hash is a method for encrypting information.
C. Incorrect. VPN is a safe network connection over Internet.
D. Correct. These are all forms of malware, which establishes itself unrequested on a computer for malicious purposes. See section 9.4.6 of "*The basics of information security*".

32 of 40

Which measure does **not** help against malicious software?

A. an active patch policy
B. an anti-spyware program
C. a spam filter
D. a password

A. Incorrect. Malware often makes use of programming faults in popular software. Patches repair security leaks in the software, thereby reducing the chance of infection by malware.
B. Incorrect. Spyware is a malicious program that collects confidential information on the computer and then distributes it. An anti-spyware program can detect this malicious software on the computer.
C. Incorrect. Spam is unrequested e-mail. It is often simple advertising but can also have malicious software attached or a hyperlink to a web site with malicious software. A spam filter removes spam.
D. Correct. A password is a means of authentication. It does not block any malicious software. See section 8.1.2.1 of "*The basics of information security*".

33 of 40

What is an example of an organizational measure?

A. backup of data
B. encryption
C. segregation of duties
D. keeping network equipment and junction boxes in a locked room

A. Incorrect. Backing up data is a technical measure.
B. Incorrect. Encryption of data is a technical measure.
C. Correct. Segregation of duties is an organizational measure. The initiation, execution and control duties are allocated to different people. For example, the transfer of a large amount of money is prepared by a clerk, the financial director carries out the payment and an accountant audits the transaction. See section 9.4.3 of "*The basics of information security*".
D. Incorrect. Locking rooms is a physical security measure.

34 of 40

Identification is establishing whether someone's identity is correct.

Is this statement correct?

A. yes
B. no

A. Incorrect. Identification is the process of making an identity known.
B. Correct. Establishing whether someone's identity is correct is called authentication. See section 8.1 of "*The basics of information security*".

35 of 40

Why is it necessary to keep a disaster recovery plan up to date and to test it regularly?

A. In order always to have access to recent backups that are located outside the office.
B. In order to be able to cope with daily occurring faults.
C. Because otherwise, in the event of a far-reaching disruption, the measures taken and the incident procedures planned may not be adequate or may be outdated.
D. Because this is required by the Personal Data Protection Act.

A. Incorrect. This is one of the technical measures taken to recover a system.
B. Incorrect. For normal disruptions the measures usually taken and the incident procedures are sufficient.
C. Correct. A far-reaching disruption requires an up-to-date and tested plan. See section 9.3 of "*The basics of information security*".
D. Incorrect. The Personal Data Protection Act involves the privacy of personal data.

36 of 40

What is authorization?

A. The determination of a person's identity.
B. The registration of actions carried out.
C. The verification of a person's identity.
D. The granting of specific rights, such as selective access to a person.

A. Incorrect. The determination of a person's identity is called identification.
B. Incorrect. The registration of actions carried out is called logging.
C. Incorrect. The verification of a person's identity is called authentication.
D. Correct. The granting of specific rights, such as selective access to a person is called authorization. See section 8.1 of "*The basics of information security*".

37 of 40

Which important statutory norm in the area of information security does the government have to meet?

A. Dependency & Vulnerability analysis
B. ISO/IEC 20000
C. ISO/IEC 27002
D. national information security legislation or regulations

A. Incorrect. Dependency & Vulnerability analysis is a risk analysis method.
B. Incorrect. ISO/IEC 20000 is a standard for organizing IT Service Management and is not compulsory.
C. Incorrect. ISO/IEC 27002 is the Code for Information Security. It is a guideline for organizing Information Security and is not compulsory.
D. Correct. National information security legislation or regulations are intended for all national governments and are obligatory. See section 10 of "*The basics of information security*".

38 of 40

On the basis of which legislation can someone request to inspect the data that has been registered about him or her?

A. The Public Records Act
B. The Personal Data Protection Act
C. The Computer Criminality Act
D. The Government Information (Public Access) Act

A. Incorrect. The Public Records Act regulates the storage and destruction of archive documents.
B. Correct. The right to inspection is regulated in the Personal Data Protection Act. See section 10.5 of "*The basics of information security*".
C. Incorrect. The Computer Criminality Act is a change to the Criminal Code and Code of Criminal Procedure to make it easier to deal with offences perpetrated through advanced information technology. An example of a new offence is computer hacking.
D. Incorrect. The Government Information Public Access Act regulates the inspection of written governmental documents. Personal data is not a governmental document.

39 of 40

The Code for Information Security (ISO/IEC 27002) is a description of a risk analysis method.

Is this statement correct?

A. yes
B. no

A. Incorrect. The Code for Information Security is a collection of measures.
B. Correct. The Code for Information Security can be used in a risk analysis but is not a method.
See section 9.1 of "*The basics of information security*".

40 of 40

The Code for Information Security (ISO/IEC 27002) only applies to large companies.

Is this statement correct?

A. yes
B. no

A. Incorrect. The Code for Information Security is applicable to all types of organizations, large and small.
B. Correct. The Code for Information Security is applicable to all types of organizations, large and small. See section 9.1 of "*The basics of information security*".

Evaluation

The table below shows the correct answers to the questions in this sample examination.

number	answer	points
1	**C**	1
2	**A**	1
3	**C**	1
4	**C**	1
5	**B**	1
6	**D**	1
7	**A**	1
8	**B**	1
9	**A**	1
10	**D**	1
11	**A**	1
12	**C**	1
13	**C**	1
14	**C**	1
15	**B**	1
16	**D**	1
17	**B**	1
18	**B**	1
19	**A**	1
20	**D**	1

number	answer	points
21	**D**	1
22	**B**	1
23	**D**	1
24	**A**	1
25	**C**	1
26	**B**	1
27	**C**	1
28	**A**	1
29	**B**	1
30	**B**	1
31	**D**	1
32	**D**	1
33	**C**	1
34	**B**	1
35	**C**	1
36	**D**	1
37	**D**	1
38	**B**	1
39	**B**	1
40	**B**	1