Practice of Information Security and ICT Security Policy

Inleiding - Belang van beveiliging en beveiligingsbeleid voor de bedrijven

Beveiliging is uitgegroeid tot een cruciaal, hoewel misschien ondergewaardeerd, investeringsgebied in informatiesystemen. Wanneer computersystemen niet werken zoals ze zouden moeten werken, lopen bedrijven die in hoge mate afhankelijk zijn van computers ernstige schade op. Hoe langer computersystemen buiten bedrijf zijn, des te ernstiger de consequenties voor het bedrijf. Sommige bedrijven die hun cruciale bedrijfstransacties geheel door computers laten verzorgen zouden bij een verlies aan computercapaciteit gedurende meer dan enkele dagen met een totale uitval aan bedrijfsfuncties geconfronteerd kunnen worden. Nu tegenwoordig zoveel zaken gedaan worden via internet en via netwerken van met elkaar verbonden systemen zijn bedrijven meer dan ooit kwetsbaar voor storingen en schade. Beveiligingsincidenten zijn in een fenomenaal tempo toegenomen.
Bedrijven moeten vaak waardevolle informatie beschermen. Systemen herbergen vaak vertrouwelijke informatie over persoonlijke gegevens zoals belastingen, financiële bezittingen, medische gegevens en functioneringsgesprekken. Ze kunnen ook informatie bevatten over bedrijfsoperaties, zoals bedrijfsgeheimen, nieuwe productontwikkelingsplannen en marketingstrategieën. Overheidssystemen kunnen informatie bevatten over wapensystemen, operaties van inlichtingendiensten en militaire doelen. Deze informatie is uiterst waardevol en als deze verloren gaat, vernietigd wordt of in de verkeerde handen terechtkomt, kunnen de gevolgen rampzalig zijn. Onvoldoende beveiliging kan ook leiden tot ernstige aansprakelijkheidsproblemen. Bedrijven moeten niet alleen hun eigen informatiebezit beschermen, maar ook dat van klanten, medewerkers en zakenpartners. Nalatigheid hierin kan het bedrijf blootstellen aan kostbare claims voor schending van privacy of diefstal. Als een organisatie nalaat om afdoende beschermingsmaatregelen te nemen om verlies van vertrouwelijke informatie, beschadiging van gegevens of inbreuk op de privacy te voorkomen, kan ze aansprakelijk worden gesteld voor onnodig genomen risico's of veroorzaakte schade. Een goed beveiligings- en beheerframework dat bedrijfsinformatiebezit beschermt, kan dus een hoge return on investment produceren.

ICT security is a management issue

As a consequence of more openness to the outside world, companies become more vulnerable for security threats. Studies show that some attacks bring along large costs. That is why companies become more and more aware that ICT security is a management problem. Actually a company needs a totally security approach. It is a must to know what are the critical resources and processes of the company and their weaknesses.

Information security and security policy
Organizations face security threats from a wide range of sources and are vulnerable to attacks such as computer viruses, hacking and denial of service attacks. Information security by technical means is not sufficient and needs to be supported by policies and procedures.

Security policies are the foundation and the bottom line of information security in an organization. A well written and implemented policy contains sufficient information on what must be done to protect information and people in the organization. Security policies also establish computer usage guidelines for staff in the course of their job duties.

System administrators and business owners have to acknowledge the fact that security threats exist and how to prevent and respond to them. Identifying and implementing suitable controls requires careful planning and participation of all employees in the organization is also vital for the success of information security management. Therefore,

depending on the company's size, financial resources, and the degree of threat, we have to set up a security policy that finds the right balance between the overreacting and the vulnerable of exposing your system to any and every hack. The objective of a well written and implemented security policy is improved information availability, integrity and confidentiality, from both inside and outside the organization.

One approach to setting security policies and procedures is suggested by the following steps :
. Identify all the assets that we are trying to protect.
. Identify all the vulnerabilities and threats and the likeliness of the threats happening.
. Decide which measures which will protect the assets in a cost-effective manner.
. Communicate findings and results to the appropriate parties.
. Monitoring and review the process continuously for improvement.

ISO 17799

ISO 17799 provides a comprehensive set of guidelines and controls comprising best practices in information security whereby it can be used as a basis to develop security policy. The ISO 17799 defines 127 security controls which are grouped into 10 sections can be used as a security checklist to assist us in defining our policy. However, not all of the controls defined will be relevant to the organization.

As part of the preparation process, a questionnaire consisting of all relevant security controls defined in ISO 17799 is created. The checklist must be designed according listing all the recommended best practices from ISO 17799 and at the same time gathering data whether it is being implemented in the organization, who is the process owner and how it is being done. A good questionnaire should have the 5W's and 1H – What ? Who ? Where ? When ? Why ? and How ?

This questionnaire will be used to understand the organization's security posture and to suggest areas where policy is needed.

IM Theme 3 : Information security

Information must be safeguarded from accidental and deliberate modification or deletion by people and also natural events which may destroy the media on which it is held. Many organizations now implement a formal information security management system or information security policy to protect their information assets.
The information management strategy will mandate that there is a security policy. This may be a policy developd in-house, or be adoption of a security standard such as BS7799.

The standard defines ten guiding principles :
1. Security policy
2. Security organization
3. Asset classification and control
4. Personnel security
5. Physical and environmental security
6. Communication and operations management
7. Access control
8. Systems development and maintenance
9. Business continuity planning
10. Compliance.

ISO 17799 standard

BS7799 is a very detailed security standard. It is organized into ten major sections, each covering a different topic or area :

1. Business Continuity Planning
The objectives of this section are as follows : To counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters.

2. System Access Control
The objectives of this section are as follows : 1) to control access to information; 2) to prevent unauthorised access to information systems; 3) to ensure the protection of networked services; 4) to prevent unauthorised computer access; 5) to detect unauthorised activities; 6) to ensure information security when using mobile computing and tele-networking facilities.

3. System Development and Maintenance
The objectives of this section are as follows : 1) to ensure security is built into operational systems; 2) to prevent loss, modification or misuse of user data in application systems; 3) to protect the confidentiality, authenticity and integrity of information; 4) to ensure IT projects and support activities are conducted in a secure manner; 5) to maintain the security of application system software and data.

4. Physical and Environmental Security
The objectives of this section are as follows : 1) to prevent unauthorised access, damage and interference to business premises and information; 2) to prevent loss, damage or compromise of assets and interruption to business activities; 3)to prevent compromise or theft of information and information processing facilities.

5. Compliance
The objectives of this section are as follows : 1) to avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements; 2) to ensure compliance of systems with organizational security policies and standards; 3) to maximize the effectiveness of and to minimize interference to/from the system audit process.

6. Personnel Security
The objectives of this section are : 1) to reduce risks of human error, theft, fraud or misuse of facilities; 2) to ensure that users are aware of information security threats and concerns, and are equipped to support the corporate security policy in the course of their normal work; 3) to minimize the damage from security incidents and malfunctions and learn from such incidents.

7. Security Organisation
The objectives of this section are : 1) to manage information security within the Company; 2) to maintain the security of organizational information processing facilities and information assets accessed by third parties; 3) to maintain the security of information when the responsibility for information processing has been outsourced to another organization.

8. Computer & Network Management
The objectives of this section are : 1) to ensure the correct and secure operation of information processing facilities; 2) to minimize the risk of systems failures; 3) to protect the integrity of software and information; 4) to maintain the integrity and availability of information processing and communication; 5) to ensure the safeguarding of information in networks and the protection of the supporting infrastructure; 6) to prevent damage to assets and interruptions to business activities; 7) to prevent loss, modification or misuse of information exchanged between organizations.

9. Asset Classification and Control
The objectives of this section are : to maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection.

10. Security Policy
The objectives of this section are : to provide management direction and support for information security.

Within each section are the detailed statements that comprise the standard.

Security analysis and security control

Introduction to information security

Information security is defined by the US National Security Telecommunications and Information Security Committee as the 'protection of information and the systems and hardware that use, store, and transmit that information' (Whitman and Mattord, 2003). Security is a vital final part of building information architecture, ensuring that information assets that the information architecture makes available to users are protected. Pipkin (2000) notes that security is a series of trade-offs : 'the greater the level of security required, the more administration and controls that are required, and the greater the tendency to reduce the ease of use. These trade-offs must be evaluated in the same way as any business asset and process.'
Legal issues such as privacy legislation require levels of security for personal information. In the UK, for example, the British Standard for Information Security is recommended for all organizations to comply with the security provisions of the 1998 Data Protection Act.
The key features of information security are :
. *Availability*. Making sure information is available to those who need it and that they can use the information when appropriate.
. *Confidentially*. Making sure information access is only available to those who require it. The opposite side to availability.
. *Authenticity and integrity*. Safeguarding the accuracy of information – is it the same as the original ? Has it been altered or corrupted ?

An information security system will have the following components :
. Data and information assets. Listing of the key assets to be protected.
. Hardware
. Software
. Policies and procedures.

Standards : British Standard for Information Security BS7799

The Plan, Do, Control, Act Model (PDCA) is a core part of the British Standard for Information Security (2002) and is illustrated in Figure 9.23.
The PDCA model offers a clear process for security management systems to be developed. The key components are explained below :
. *Plan*. Establish policy, objectives, targets, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
. *Do*. Implement and operate the security policy, controls, processes and procedures.
. *Check*. Assess and, where applicable, measure process performance against security policy, objectives and practical experience and report the results to management for review.
. *Act*. Take corrective and preventive actions, based on the results of the management review, to achieve continual improvement.

The security analysis process will include an investigation of any existing documentation relating to security. This will include assessing any security policies in place, documented security breaches and incidents and information from information security controls already in place.

Controlling information security

In these chapters we saw that standards are available on which to base an information security policy, such as BS7799 to help structure the approach to defining security. It is clearly in organizations' interest to protect their information, as a valuable asset. Furthermore, in many countries, it is now required by law to put in place security controls. For example, in the UK the Information Commissioner suggests these questions that an organization needs to ask to ensure it has adequate security :

1. Does the data controller have a security policy setting out management commitment to information security within the organization ?
2. Is responsibility for the organization's security policy clearly placed on a particular person or department ?
3. Are sufficient resources and facilities made available to enable that responsibility to be fulfilled ?

The concept of a data controller is described in Chapter 12 in the section on Privacy law. As we saw in Chapter 9, the security policy typically sets out two areas : controlling access to information and achieving business continuity.
Controlling access to information is required to manage information theft or deliberate or accidental deletion of information. More detailed questions posed by the Information Commissioner to assess controlling access to information are :

. Is access to the building or room controlled or can anybody walk in ?
. Can casual passers-by read information off screens or documents ?
. Are passwords known only to authorized people and are the passwords changed regularly ?
. Do passwords give access to all levels of the system or only to those personal data with which that employee should be concerned ?
. Is there a procedure for cleaning media (such as tapes and disks) before they are reused or are new data merely written over old ? In the latter case is there a possibility of the old data reaching somebody who is not authorized to receive it (e.g. as a result of the disposal of redundant equipment) ?
. Is printed material disposed of securely, for example, by shredding ?
. Is there a procedure for authenticating the identity of a person to whom personal data may be disclosed over the telephone prior to the disclosure of the personal data ?
. Is there a procedure covering the temporary removal of personal data from the data controller's premises, for example, for staff to work on at home ? What security measures are individual members of staff required to take in such circumstances ?
. Are responsibilities for security clearly defined between a data processor and its customers ?

Business continuity planning

Managing for business continuity or disaster recovery seeks to control disruption if the methods for protection of information are insufficient. Disruption can result from malicious deletion of information through a hacker or employee or as a result of a virus as described in the Managing computer viruses section later in this chapter. Disruption can also occur through so-called 'acts of God'. Here natural hazards such as fire, flood or storm cause computers holding information to be destroyed. Acts of terrorism can also destroy computers and the information they contain. Organizations need to plan for business continuity in the event of a major incident that destroys the working environment and/or IT by ensuring that if information or technology is lost or destroyed, the business can continue with the minimum disruption possible. This requires back-up

of all data, often on a remote site which won't be affected by the same incident and the ability to deploy new servers and PCs in a new location if required. The approach used is known as 'business continuity' or 'disaster recovery planning'. An example of a plan which is publicly available is for the Massachussetts Institute of Technology (http://web.mit.edu/security/www/isorecov.htm). This plan shows how an assessment of risks is performed and the action that occurs in the event of a problem :

1. Detect and determine the start of a disaster condition
2. Notify persons responsible for recovery
3. Initiate the Institute' Business Continuity Plan
4. Activate the designated hot site
5. Disseminate Public Information
6. Provide support services to aid recovery.

European data protection and privacy law requires that customer and employee information is adequately protected. The UK Information Commissioner gives guidelines based on asking these questions to check that protection measures are adequate to ensure business continuity :

. Are the precautions agains burglary, fire of natural disaster adequate ?
. Is the system capable of checking that the data are valid and initiating (automatically scheduling) the production of back-up copies ?
. If so, is full use made of these facilities ?
. Are back-up copies of all the data stored separately from the live files ?
. Is there protection against corruption by viruses or other forms of intrusion ?

Security audit

The role of audits

How does the management know if security measures of Information systems are effective. To answer that question companies should apply audits on a elaborative and systematic basis. A security audit controls which measures are taken with each of the systems separately and checks efficiency.
The auditor interviews key persons that use and control a specific Informationsystem. He questions the use, the taken procedures, the security, the measures in application, procedures for safekeeping the allround integrity and control methods. A prioritylist of weak spots in the security is made up in the audit and the estimated chance of failures caused by those weak spots

Hoe weet het management of de beveiligingsmaatregelen bij informatiesystemen effectief zijn ? Om deze vraag te beantwoorden moeten organisaties uitgebreide en systematische audits uitvoeren. Een EDP-audit gaat na welke maatregelen bij de afzonderlijke informatiesystemen zijn genomen en beoordeelt de effectiviteit ervan. Bij een audit baseert de auditor zich op kennis van de exploitatie van ICT-voorzieningen, de fysieke locatie en haar faciliteiten, de gebruikte netwerkverbindingen, de beveiligings-systemen, de beveiligingsdoelstellingen, de organisatiestructuur, het ingezette personeel, de handmatige procedures en de toepassingen.
De auditor interviewt meestal de belangrijke personen die een specifiek informatiesysteem gebruiken en beheren en vraagt dan naar hun gebruik en de door hen in acht genomen procedures. Er wordt gekeken naar beveiliging, maatregelen in de applicatie, procedures ter waarborging van de algehele integriteit en beheermethoden. De auditor moet de stroom van de transacties door het systeem nagaan en tests uitvoeren en kan, waar nodig, geautomatiseerde auditsoftware gebruiken.
EDP-audits moeten de gebruikte technologieën, procedures, documentatie, training en het personeel beoordelen. Een zeer grondige audit zal zelfs een aanval of een ramp

simuleren om de reactie van de technologie, het personeel van informatiesysteem-afdelingen en de zakelijke medewerkers te testen.
Bij de audit wordt een ranglijst opgesteld van alle zwakke plekken in de beveiliging en een schatting gegeven van de kans dat hierdoor een probleem ontstaat. Vervolgens wordt de financiële en organisatorisch impact van elke bedreiging vastgesteld. Figuur 9.6 is een voorbeeld van een door een auditor opgestelde lijst van zwakke plekken in de beveiliging van een leningssysteem. Hierin is een gedeelte opgenomen waarin het management wordt geattendeerd op dergelijke zwakke plekken en waarin zij hierop kunnen reageren. Van het management wordt verwacht dat ze een plan kunnen ontwerpen om duidelijk zwakke plekken in de beveiliging te verbeteren.