Walter Verhoeven
WESO / LIFE

Security Management Practices

What management need to do before we can make WESO's system secure

»Become aware
»Know what you have
»Implemet security management practices

This presentation follows the guidelines set up by "The International Information Systems Security Certification Consortium" also known as (ISC)² ® and targets ISO® 17799 Information Security Management

About this presentation

We have created this presentation to create awareness for security threats and show you how to plan for them. This presentation helps me to assist the upper-management of WESO in:

1. Securing their resources
2. Provide guidelines as to what infrastructures are needed
3. Regulate the use of IT Systems
4. Regulate the functional requirements on the software that is going to be Created for and or used by the WESO group.
5. Become ISO certified

The information that I will present in this presentation comes from ISO Guidelines 17799.2002, 2 books "**Information Security Management Handbook"** and "**The Information Systems Security Officer's Guide"** as well as some life experience**.** This presentation is conform to the current guidelines as proposed by "The International Information Systems Security Certification Consortium, Inc.", or (ISC)².

ISC is a non-profit organization, incorporated in the Commonwealth of Massachusetts, based in Palm Harbor, Florida. (ISC)² and is dedicated to:

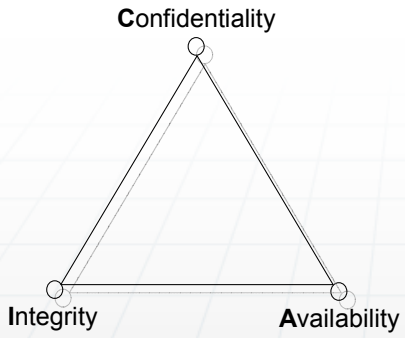
1. Maintaining the CBK for information security
2. Certifying industry professionals and practitioners under an international standard
3. Providing education
4. Administering certification examinations
5. Ensuring the continued competence of credential holders

ISC, like ISO, is an international recognized certification authority, you can find more information about them at www.isc2.org and www.iso.org

This presentation targets the certification for ISO 17799. Abiding to the recommendations made in this presentation will bring a good step closer in becoming certified. However, there are topics in the 74 page ISO 17799 specification that are not included in this presentation (like §8.4 Housekeeping ,§9.5.6 Duress alarm to safeguard users ,§9.5.7 Terminal Time-out).

Securing the System

C.I.A.-The „Big Three“

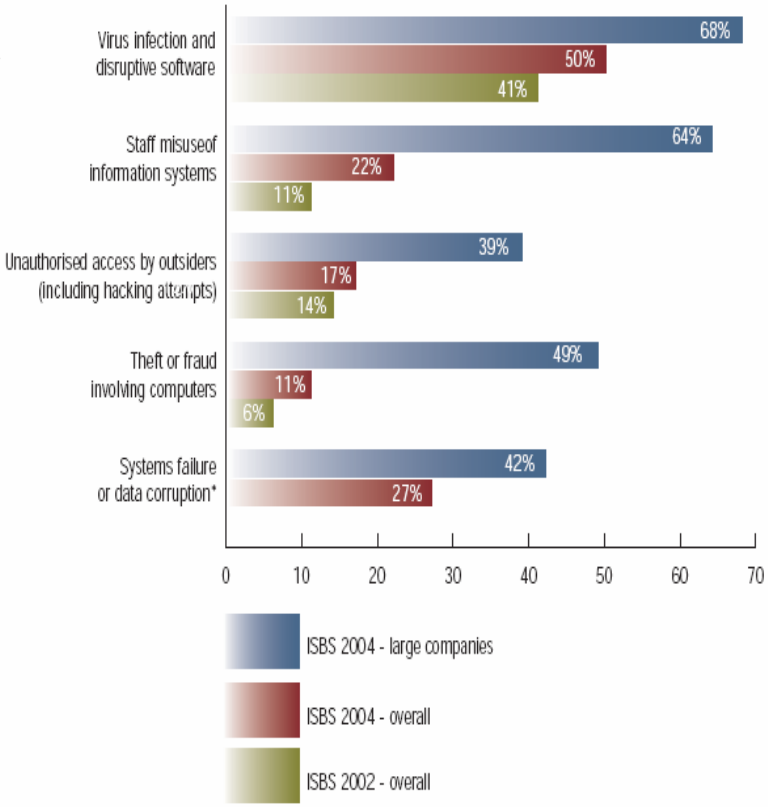


- Confidentiality: could the date have been disclosed to some one, who has gained access
- Integrity: could the data have been altered, does the software validate user input
- Availability: can someone destroy my data or stop my Network from functioning

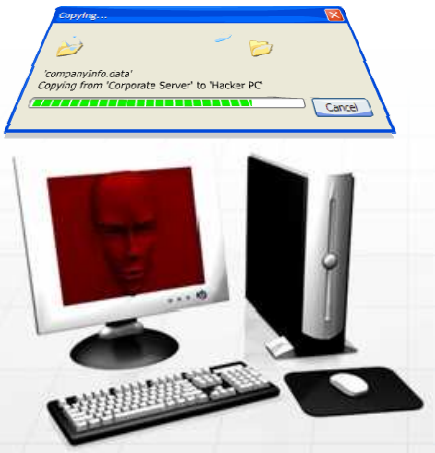
Securing a system is crucial to WESO's operational needs. There are about a few subjects one must consider, however the big three are:

1. **Confidentiality** as in who gets to see what.
2. **Integrity** as in does the software I use save the date I enter correctly and, does my hardware save the data or does it corrupt them.
3. **Availability**, can I access the data
   - where I need it
   - when I need it
   - how I need it
   - and is the speed in which it is offered to me acceptable.

What do I do when hardware or software fails



Confidentiality



- Protects data from unauthorized disclosure
  - Physical security
    - Clients/servers: who has access to the computers and how to protect them
    - Backup media: what passwords to use for backup media and where to store them

•What will WESO do to implement that the data it has does not fall in the wrong hands. Can some one walk into the building an take papers from a desk, snatch a Backup tape, plug-in a USB Drive and copy data, walk away with a server?

•Who will have access to computers?

•How will backup media be stored?

•Do all computers lock when employees leave the systems unattended!?

•Will WESO implement a 2 phase security where only certain computers can access certain data, regardless of the user who is logged on. Will it use key-cards as well as user passwords. Or will it use bio-metric security like thumb-prints.

•What are the procedures for adding/ removing a computer and / or a user to the network.

•How will computers be sanitized before removal or handling by non authorized or external personnel, an example: A Hard disk/ laptop needs repair, someone from HP will come and fix it, what will he do with these parts; RAM as well as hard-disks hold data. This person could try to load/install his favorite management or testing tools.

•When accessing secure data over the world wide web, will the user get prompted for a user name, password, and a variable personal question.

•When do we lock a user account after false identification and for how long. How do we go about unlocking them.

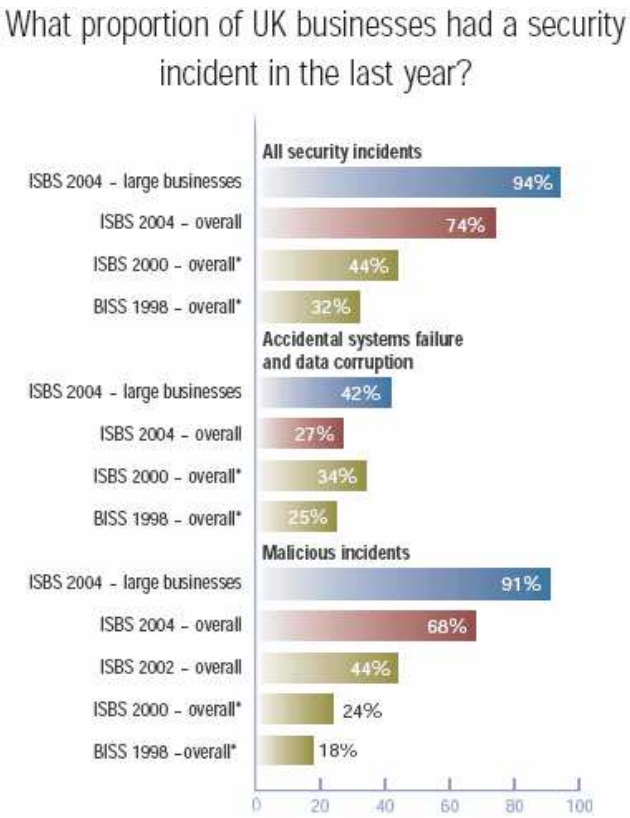
Integrity

- Access control
  - Local/ Remote access
  - User IDs and Passwords
  - Data objects (Files, Database tables) using runtime access control
  - Cable shielding
  - Data encryption
    - SSL/TLS network encryption
    - VPN (**V**irtual **P**rivate **N**etwork)
  - Perimeter Defense
    - Firewalls
    - Virus wall
    - IDS (**I**ntrusion **D**etection **S**ystems)

System integrity is everything, imagine someone can go into the system and alter the bank account or amount for a transaction that has been approved and pending transfer. After the transaction took place the person could restore its original contents and / or crash the system. Will we ever find out. Do we even suspect it happened?

1. What levels of data/file access will need o be implemented.
2. How to enforce user name and passwords.
3. How to monitor data access and who reeds these reports.
4. What level of encryption is needed on the LAN and what level of encryption is needed on the WAN.
5. What resources are going to be made available for monitoring the network and it's data.

"The 2004 Department of Trade and Industry Information Security Breaches Survey" (UK) results clearly show that 91% of departments have some sort of malicious security incident per year.



Availability

- Ensures the system is available when needed.
  - Fault tolerance
    - Hardware redundancy
    - Software replication
  - Performance tuning
    - Network bandwidth utilization
    - Protection from Denial of Service (DoS) Attacks

How will we solve the following objectives if in fact they are desirable

1. What needs to be made available in relation to backup/ standby hardware

   It is possible to have virtual servers, this trick allows the network to show one server, an example: a web server in using several machines. This can be a virtual server or better load balancing.
2. What response times are acceptable in case of problems and how to escalate it. A vital part stops functioning say a IDS or a Firewall what do we do.
3. How much resources will be made available for improving and monitoring the availability to the companies IT infrastructure.

Who is Responsible

- Management
  - Management is responsible to ensure security by making plans. It is the IT-staff's responsibility to implement it.
  - What security structures are needed, and will it be practible enough for the staff to be accepted.
  - A solid security administration is implemented in a top-down approach.

Management needs to be informed about the available technologies as well as possible threats so that it can make the appropriate budget and resources available. The IT staff assists management with the implementation as well as making methods available so that monitoring the fulfillment of the requirements is possible and management can validate that the objectives have been met.

Users must be monitored and trained; this is to make sure that they can be productive and feel protected by the system, not restricted.

Make sure that responsibilities for the protection of individual assets and for carrying out specific security processes are clearly defined and assigned to a individual.

Every Security policy has an owner. The owner is responsible for its maintenance and its review according to a defined review process.

Do these processes ensure that a review has taken place in response to any changes affecting the basis of the original assessment, example: a significant security incident, new vulnerabilities or changes to organisational or technical infrastructure.

Security Goals

- Strategic – Long-term
  - Where do we want to get to in the years to come
- Tactical – Medium-term
  - What requirements are needed for new products that are in the pipeline
- Operational – Day-to-Day
  - What needs to be done now to maintain system integrity

A good solid security policy should address all of these topics.

Long Term

•What does WESO want to do in the future, what services are we going to need and give in say 2 years or more and does the system allow for growth?

Medium-Term

•What will a product lifecycle look like, what security issues become important at the various stages of the product.

•What are the product lines WESO would like to implement and what are the security needs for this product

Day to day

•Maintaining operations

•Making sure the firewall and viruswall can protect us from current threats

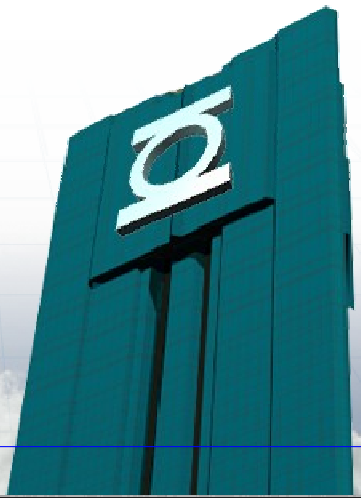
•Users on the system have sufficient rights to perform their tasks

•Maintaining a secure system access.

•Reporting issues back to the control owner for review

Organizational Requirements

- Understand specific organizational security requirements
- Confidentiality needs
- Management style and organizational culture

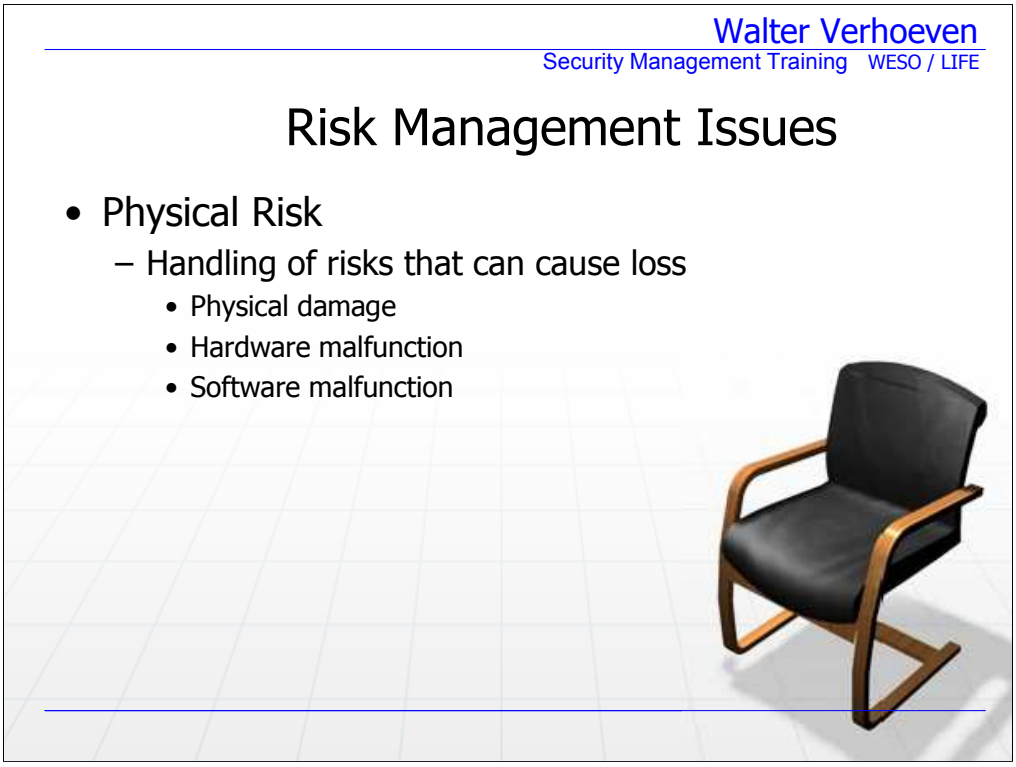


What type of organization is WESO and what are the requirements on confidentiality.

We must show that there is a management forum, and ensure that there is a clear direction and visible management support for security initiatives within the organisation.

How do we make sure that the security goals are in sync with WESO's objectives and that they support WESO's management style. If the users do not accept or understand the policies they will end up not implementing them and may even revolt.

We must take into consideration all de different nuances that make up WESO as a company.



Physical Damage

Make sure that all risks that can cause loss in regards to physical damage, computers, hard disk, backup tapes, network equipment, the building, electricity supply etc. are known.

Hardware malfunction

A disk controller could be writing incorrect data to disk, how do we address this? What if the power lines get hit by lightning. Look at what physical components are critical and plan for a loss.

Software malfunctions

Do we have the appropriate service packs, can the installation of a service pack stop other devices or software performing within its normal parameters. Install an other Java, Visual basic, or .Net version and software can stop performing with in its regular parameters. Who will test the updates and what will be its certification procedure.

Further more the users must have a central point where these malfunction related issues can be registered, tracked and managed.

Risk management issues

- Human Risk
  - Malicious attack
    - Virus
    - Hacker
    - Member of staff
  - Espionage and theft
    - What is the value one can suffer a loss from through Espionage or theft
    - What is the value of disclosure to my competitors
  - Human errors
    - Deletion
    - Wrong/ invalid data entry

When analyzing a threat evaluate the appropriate priorities as well as to what the cost of a particular response would be

Malicious attack

Malicious attacks is more than hackers and viruses, it could also be an employee who wants to harm the credibility of someone in the organization or as revenge against the organizations management.

Espionage and theft

•Can someone sell data or proprietary software to other organizations.

•What would be of interest and how difficult is it to get to it.

•Can password protecting a document help?

http://www.lostpassword.com/ sells a office password recovery for $150 to anyone with a credit card, or have a look at http://www.webattack.com.

Even worse the US Governments High Tech Crime Network at http://www.htcn.org/ offers the latest tools for free.

Human errors

•Some possible user errors

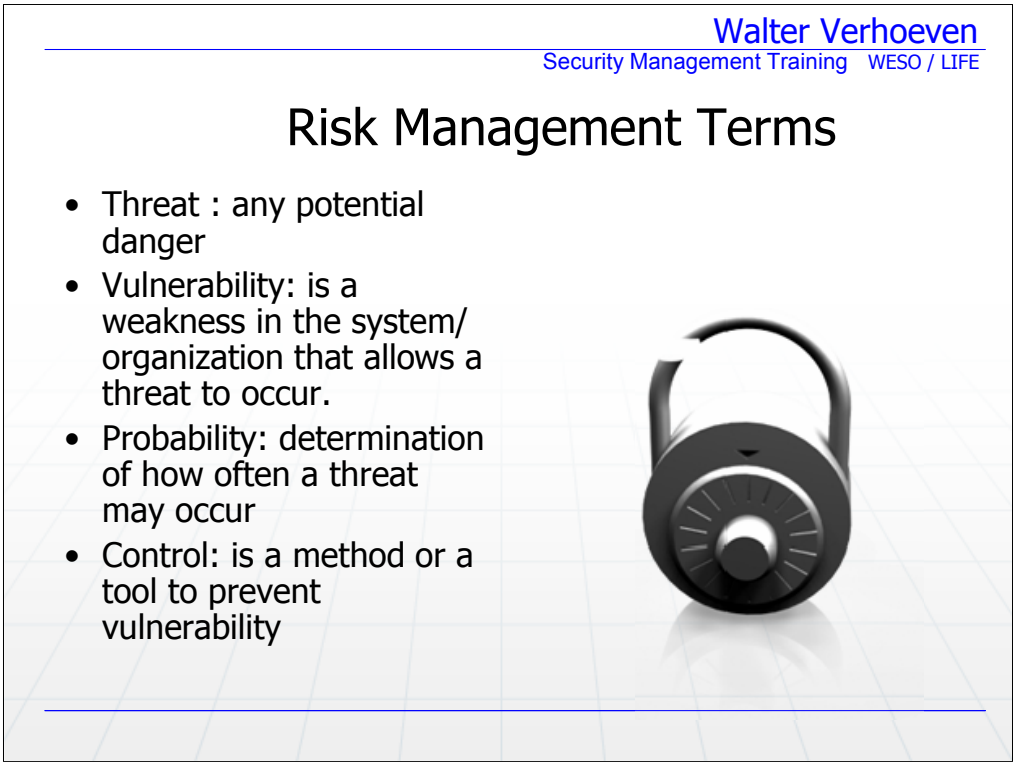
•Document loss due to deletion or overwriting.

•Unintended document changes

•Submitting data to an application or web page that was incorrect or incomplete

•What needs to be protected and how can it be protected?

•How can the user request the restoring of a file?



Threat

Anything that can potentially cause the organization or the system from functioning as it was attended or that could cause a loss.

According to the Deloitte Touche 2003 Global Security Survey of worldwide financial services institutions, over a third of banks and financial services companies surveyed reported a security breach in the last year. Of the 39% who admitted their systems had been compromised, 16% were due to external attacks, 10% internal breaches and 13% both. (www.silicon.com and BNA's Internet Law News, 14 May 2003) . Remember admitting to a security breach for a bank is not that good for their reputation; what would the real numbers be?

Vulnerability

This can be a missing virus definition in your antivirus software, a weak password, a broken lock on the gate, or a photocopy machine. “The National Institute of Standards and Technology” at www.icat.nist.gov allows anyone to see the latest found security risks in their ICAD Database http://icat.nist.gov/icat.cfm . Querying this database on 5.06.2005 were 41 recorded threats that have little or no means to avoid them. If you would like access to a system then this is the how-to guide in doing so.

Probability Determination

How likely is it that a vulnerability is going to be exploited.

Control

After having analyzed the probability of an security exploit or any other kind of threat one needs to make sure that the safeguards designed to prevent it are implemented.

Risk Management Options

- What is the Risk
  1. Can we accept it
  2. What is the likelihood of it occurring
  3. Cost of controlling
  4. Can we reduce/mitigate the risk
  5. Can we reduce the likelihood of it occurring
  6. Assigning the risk to someone (insurance, warranty,..)

Acceptance:

Can we accept the risk, sometimes IT staff members will change, they will remember system passwords, can we change all passwords, the passwords on tapes we can't.

Likelihood

An example:

- How likely is it that the building will be hit by a meteorite and how can we prevent it
- What are the chances of my administrator copying the system and then going to sell it to the competition

Cost

What would it cost to implement all the controls needed for a risk not to occur versus all the costs of when a risk occurs. An example:

What if a hard disk crashes, data gets corrupt.

Costs of controlling

1. What is the replacement cost €120
2. What does it cost to have backups €30,000
3. What does it cost to restore the data €15

Costs of not controlling

1. What is the replacement cost €120
2. Re-install the Server using server install €230
3. Re-entering this years data from paper archives €?

Legal Responsibility

- Due Care
  1. Taking responsibility for security
  2. Demonstrating the taking of responsibility
     - You must have planned for threats and vulnerabilities
     - You must document the process
- Due Diligence
  1. Ensure continually monitored and updated controls
  2. Revisit and ensure threats and analysis are correct
  3. Ongoing risk assessment and documentation

Most Legal entities will be satisfied if you can prove that you “Due Care” and “Due Diligence”.

Without this you will be in trouble if it ever goes to court.

You must show that:

1. You formed a team
2. Evaluated loss
3. Implemented controls.

We have started “Due Care” by having this presentation. We have taken responsibility, we are going to plan for threats and most important we documented doing so!

If WESO plans to obtain the ISO 17799 certification it shows that it takes security serious and helps the company implementing a good IT infrastructure

Risk Assessment Team

- Who should be on the team
  1. Upper Management
     - If no support from upper management exists, implementing it will never work.
     - This manager must have signing ability, things are going to cost money.
  2. Include Multiple Departments and Roles
     - Not just IT or persons close to the IT department
  3. Accept all Input
     - Anonymous input like questionnaires can help
  4. Document all Proceedings

Management

Management must understand the whole security concept.

Remember management sets the tone, implementing something in a company is a Top-Down approach.

Multiple Departments

Having a member of every part of the organizational tractor in place will allow you to get the “best” solution for “All” threats as the person working with an asset on a daily basis knows its weaknesses best.

Document

Documenting the proceeding in a protocol is a great memory refreshment as well as it helps to assign tasks. Without the documentation we can not prove the “Due Care” and “Due Diligence” and legal entities my not cover or accept any clams.

Assessing Risk, an Overview

- Quantitative Risk Assessment
  - Assigning a numerical value to the likelihood and extend of each risk
    - How often a particular risk is likely to occur
    - If it occurs, how much will it cost?
- Qualitative Risk Assessment
  - No numbers just comparisons
  - Helpful in ranking risks
    a. List of all the risks
    b. Take input from the various departments
    c. Decide if the risks are bad or not a big deal
    d. Rank the particular risks

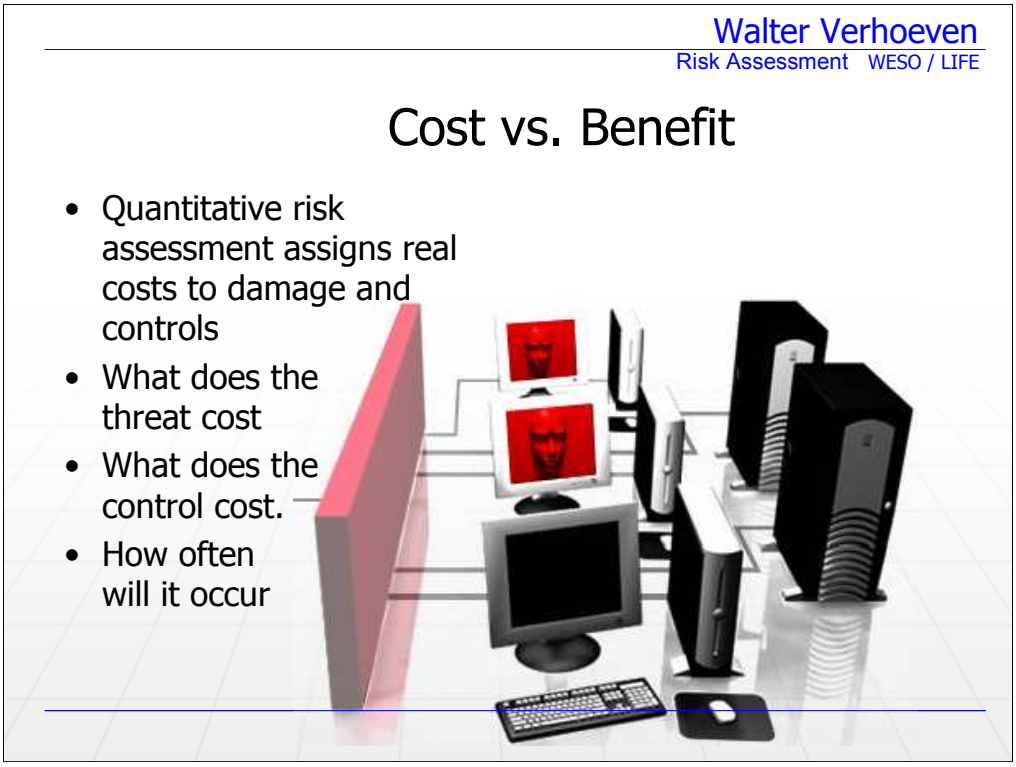
How do we asses risk?

We know that we have to asses risk, we must find out what is important and then what are we going to do about keeping it secure and available.

The 2 primary techniques to do this are **Qualitative** and **Quantitative** Risk Assessment.

Qualitative does not mention numbers it focuses on the risk ranking.

Quantitative is all about assigning scope and values to a risk.



A good example is a virus-wall. Virus-walls look for viruses before they are saved to a file on the network, so before your “Norton Anti Virus” can check it. What would it cost to have one? Approximately 3000 euro. What does a virus cost our network and all it’s data? CMS on their website offer a virus calculator (http://www.cmsconnect.com/Marketing/viruscalc.htm). Here a virus attack can be simulated as to what the productivity loss and salary cost would be. Usually it comes down to loosing all of today's email as well as 1 to 10 days of system downtime. Not to underestimate are the phone calls and emails from clients who’s antivirus system did find this virus. Or the calls from other system administrators complaining that you are infecting their servers.

The US based “Computer Security Institute” conducted a survey of 538 computer security practitioners in the United States. Their results revealed that 85% of respondents had detected computer security breaches within a twelve-month period. The 35% have listed a financial impact report of $377,828,700 in financial losses. (2001 Computer Crime and Security Survey. "Computer Security Institute (www.gosci.com).

More than 87% of all viruses enter the enterprise via email. Email has evolved beyond communication to become a business critical application. If email goes down, vital links to customers and vendors go down with it, and business grinds to a halt. (ICSA Labs Sixth Annual Computer Virus Prevalence Survey 2000 (www.ICSA.net).)

Cost vs. Benefit

- Process is Intensive
  1. Substantial information gathering
     1. Cost Calculations
     2. Probability analysis as to how often a particular threat occurs.
        a. assign a value to a control
        b. Determine cost effectiveness of a control
  2. Be aware of gray areas

The cost vs. benefit analysis will take a lot of time as you need to collect tons of information and set up all the spreadsheets; the calculations on the spreadsheets are not to be underestimated either.

This will then allow us to assign a value to a control and the cost effectiveness. It makes little sense to spend 5 euro on a 1 euro resource. However you will not know what a resource or control cost until you created the spreadsheets.

Gray Areas

Repairing the corporate website from backup tape after a Hacker altered the site is not the cost. The cost is what did he do with the data, what legal ramifications will this have on the company, and last but not least, what is the cost of “lost image”.

When defining the cost of a control make sure we look at more than what we are protecting ourselves from.

Single Loss Expectancy

- Quantitative Risk Assessment
  - Calculate exposure
    - Assign a value to each asset
    - Determine % of loss for each realized threat
      - Exposure Factor (EF)
  - Calculate the loss for a single threat occurrence
    - Single loss Expectancy (SLE)

      SLE = Asset Value X EF

Create a spreadsheet where you list the value of each individual asset.

Determine how much the loss would be an case an event materializes. The threat, when managed, for example a disc controller is not functioning and it writes bad date to all drives (including the replicated drives), would cost replacing the controller, restoring some files and re-entering others. This makes up the Exposure Factor or EF.

To calculate the single loss one would take the value of an asset, multiply it with the exposure factor and we have the Single loss expectancy or SLE.

So a 50.000 dollar file server (server + data) burns down. If the exposure facture or how much data is lost would be 50%, the single loss expectancy is 50.000 * 50% = 25.000

Quantitative Annual Loss Expectancy

- Calculate the annual probability of a loss
  - Suspected Rate of Occurrence (SRO)
    - An estimate of annual probability a stated threat will be realized
    - Will be different for ever type of identified threat
- Calculate the annual estimated loss of a specific realized threat
  - Annual Loss Expectancy (ALE)

    ALE = SLE x SRO

Asset	Risk	Value	SLE	SRO	ALE
Building	Fire	$700,000	$425,000	.20	$85,500
File Server	Disk Crash	$50,000	$25,000	.20	$5,000
Sensitive Data	Stolen	$200,000	$180,000	.70	$126,000
Internet Connection	Down	$40,000	$40,000	.80	$32,000

Budgeting

The annual expectancy of Quantitative Risk Assessment informs the budget persons as to what amount of resources need to be made available.

Risk assessment

Having a central point as to where users report/register the errors allows te “controls owner” to analyze its effectiveness and correct SLE,SRO and with it the ALE.

Documenting all errors and assigning the errors to a resource and control is vital for having a reliable risk assessment.

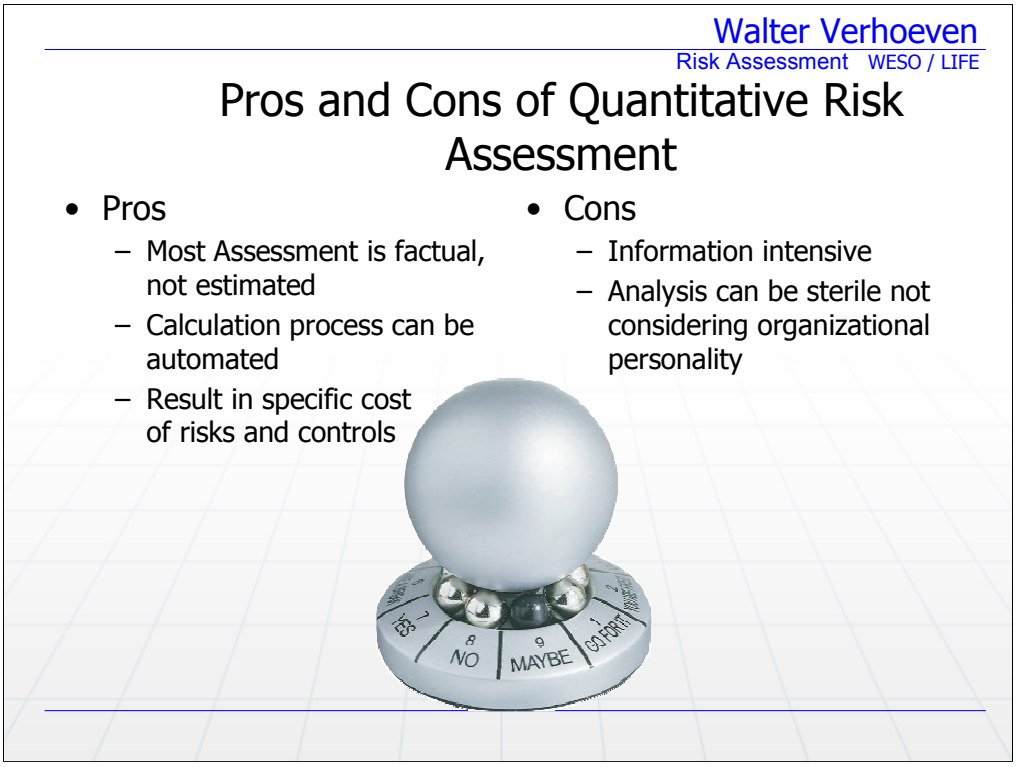
Calculating Overall Risk

Asset	Risk	Value	SLE	SRO	ALE
Server Room	Lightning	1.000.000	800.000	0.20	160.000
File Server	Disc Crash	50.000	25.000	0.20	5.000
Sensitive Data	Stolen	200.000	180.000	0.70	126.000
Internet Connection	Down	40.000	40.000	0.80	32.000

- Locate the most serious threat.
- Calculate the cost of a control that allows us to minimize the threat
- See if the benefits of the control outweigh its costs

So if we expect lightning to hit the server room every 5 years and the cost of items in this room is 1 million, the annual budget set aside for this threat would have to be 160.000. However the technologies in our server room would surely not cost 160.000 5 years from now.

This allows us to prioritize our attention to the threats that cost us the most, and see if letting a threat occurs is more cost effective than implementing controls against it.



Pros

We have done research, have experience with the resources and risks, this is what we base our estimates on.

Automation

You can automate this process using spreadsheets, correcting the SLE and SRO to reflect our exposure over time.

Result

With this spreadsheet we can sort as to which risks hit us hardest and take appropriate actions on those. This will let us compare what controls we can use to face a possible threat; we will also have the costs associated with them. This assists us with the costs assessment over a particular control.

Cons

It is intensive. We will need to collect tons of information before we have all data needed to make an assessment. Just imagine how many assets WESO will have and all the particular threats associated with them.

Number crunching does not reflect good-will or corporate image and perception. Loosing the IT room might cost a lot, however someone who hacks into the webserver altering the corporate website could: 1. cost more in non monetary values and 2. take a lot of time and resources to restore.

Qualitative Assessment

- Does not assign cost values to risk
- Risks are ranked by impact and likelihood
- Summarize each risk and its associated control
- Resulting analysis shows you which controls provide you with the most protection

Pros

- Requires few calculations
- Capitalizes on knowledge of staff

Analysis for someone stealing Data

Source	Severity	Likelihood	Control	Effectiveness
Development	3	0.50	Honey pot	8
IT Manager	7	0.60	Firewall	9
Operations Manager	9	0.80	Firewall	7
System Administrator	9	0.90	IDS	8
Accounting	10	0.01	User Rights	10
House keeping	2	0.10	Door Lock	5

Cons

- Assessment is very subjective
- No associated cost of losses and controls
- Difficult to automate

Pros

1. It allows **you** to get input from the staff on what **they** feel is most important.
2. It allows **you** to ask group members what threats affect **them** the most, HR, accounting and IT will surely have different opinions.

Cons

1. As you are not assigning values to the risks you end up getting information that is contradictory. One department , say software development thinks that someone stealing the companies source codes is not a big deal, “it will take years to understand 2 million lines of code and by then we have improved our product” whereas the IT staff thinks it is a big threat as it has “hard coded access codes to the system” as well as the formulas and other WESO specific know-how.
2. One does not have any costs associated with a **loss** or with the **control**.
3. It will be difficult to automate the evaluation.

Source	Severity	Likelihood	Control	How Effective
Development	3	5	Honeypot	8
IT Manager	7	6	Firewall	9
Operations Manager	9	8	Firewall	7
System Administrator	9	9	IDS	8

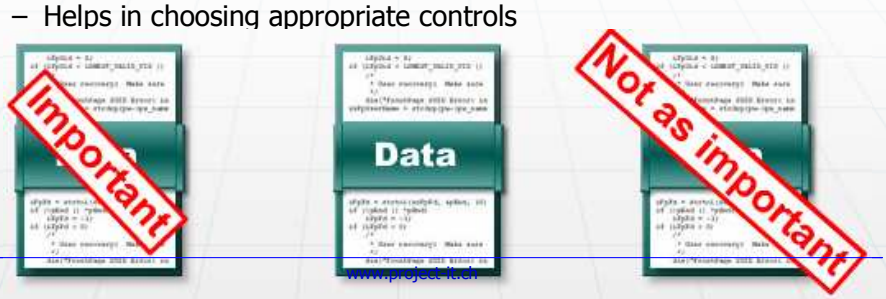
Selecting Controls

- Choose appropriate controls based on qualitative and quantitative assessment to mitigate risk
- The value is always related to the amount of loss a control prevents
- Always explore alternate options for expensive controls
  - Assignment (insurance)
  - Avoidance
  - Accept it/ let it happen

-/-

Data Classification

- Controls can be expensive in overhead, administrative or monetary resources
- Only protect what must be protected
- Data classification
  - Identifies what data in the organization is valuable
  - Satisfies legal or regulatory requirements
  - Helps in choosing appropriate controls



1.It can take a lot of time to control the use of data, time is expensive just like hardware is. Remember that your staff must accept the controls for them to work. When they are in stress they will want to be able to do things fast, also keep it simple and / or transparent to the users.

2.Do not lock data that does not need to be locked.

3.Too expensive for the company and too frustrating for its users.

4.Classify data using different points of view in regards to internal importance as well as the importance to the competition.

Classification Criteria

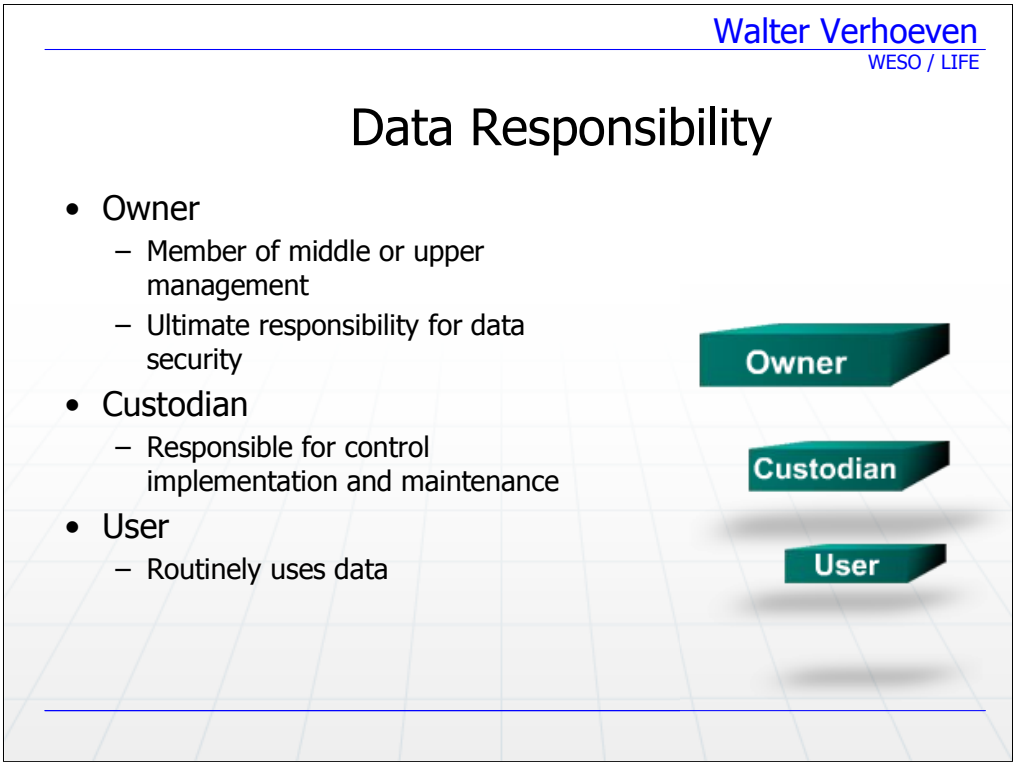
- Value or usefulness of data to our company as well as the value of the data to the competition
- Age of the data
- Laws and regulations
- Personal association

1.Just how valuable is the data to us and what can others do with it.

2.Old software designs, say 3 years old, will not be as important as the designs of the latest release. What is the relevance of a contract that was terminated 20 years ago?

3.What law and regulations must we satisfy. Say WESO would like to sell its product in the US, what do we need to ably to, will it be the same for the UK or the Netherlands. Do these rules/ regulations conflict with each other?

4.The personal data of a corporate CEO is always more important than the information of someone in housekeeping. This is true for the competition as well as internal parties. What would you think about “head-hunters” being able to identify and snatch away your key-innovators?



Owner

The owner of the data is always someone in charge of a department or in upper management, the data entry clerk or the CEO's secretary do not own the data.

Custodian

Typically someone from IT that makes sure that the data is maintained and regulated as specified by the data owner.

Users

The users of the data work with the data with in the limits of his or her access control to the data.

The user uses the data based on the rules enforced and monitored by the custodian that where implemented using the requirements setup by the data owner.

It is imperative that

1. security controls are in place (for software and hardware)
2. methods of reporting malfunctions are implemented
3. access logs are being kept
4. security breaches are reported
5. a formal disciplinary process is in place for employees who have violated organisational security policies and procedures

Security Policy

- The security policy is the base for all security controls.
  - The policy represents the management position on security
    - include
      - Statements of expected performance
      - Consequence of noncompliance
    - Should be strategic in nature, abstract, and long term.

This is the first document that states the entire content that WESO has towards security

This is the starting point that is crucial before **we** can start to implement any type of security controls.

Security Policy Types

- Regulatory
  - Mandatory to satisfy legal or regulatory requirements.
- Advisory
  - Strong statements that specify unacceptable behavior and associated consequences
- Informative
  - Explains organizational strategies and behavior

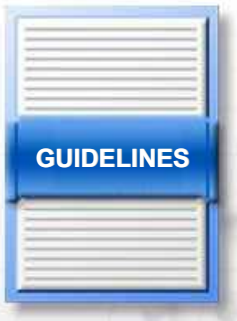
What are the positions that WESO must fulfill as part of regulatory requirements for it to do business.

These are directives, they state **what** you must do, not **how** you must do it.

Standards can also tell how programs are allowed to operate by allowing certain features and forbidding others.

The ISO 17799 standard is an example of this. It tells you what you must do and not how you can do it. It is also abstract so that it can be applied to several types of organizations and stays independent of technology advancements.

Guidelines



- Recommended action or guide
- Typically not mandatory
- Shows general direction but is flexible enough to allow alternate means of achieving it.
- Provide details on how to implement standards

Guidelines need to show us how to fulfill the standards. An example is the guideline of how to program for the windows environment. Guidelines usually do allow several procedures on how to achieve this.

Procedures

- The "how to" document
- Contains step-by-step instructions
- Specific to well-defined areas
- May have multiple sets of procedures that can be used to satisfy one guideline

These how-to documents describe how the goals need to be implemented.

An Example: what are the management authorisation procedures going to be for any new resources. This should include all new resources such as staff, hardware and software.

There should be a cross-functional forum of management representatives from relevant parts of WESO's organisation to coordinate the implementation of the various information security controls.

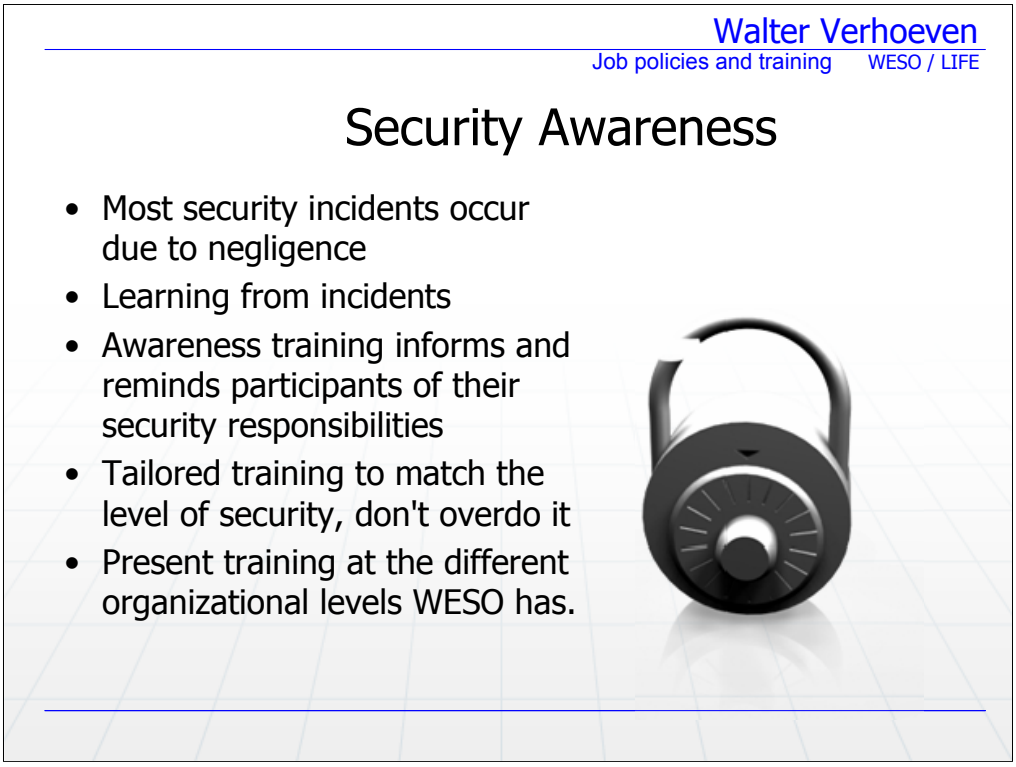
Employee

- Hiring Practices
  - Background check
  - Drug testing
  - Security clearance
  - Nondisclosure agreements
  - Job description
    - Accountability
    - Physical access
    - Logical access
- Termination Practices
  - Revocation of privileges
  - Security escort
  - Exit interview
    - Good information
    - Ask security questions
    - Sign security documentation

Are employees going to be asked to sign a confidentiality or non-disclosure agreement as a part of their initial terms and conditions of the employment. Does this agreement cover the security of the information processing facility and organisation assets as well has her/his responsibility in it *(§6.1.3 of the ISO 17799 standard)*.

Do terms and conditions in the employment contract specify the employee's responsibility for information security *(§ 6.1.4 of the ISO 17799 standard)* These responsibilities might continue for a defined period after the end of the employment, is this clear to the employee and is this enforceable.

Mandatory vacation blocks of minimum one week allow for outside auditors to audit the employee's activities as well as a regular job rotation to reduce the risks of human error, theft, fraud or misuse of facilities.



Negligence

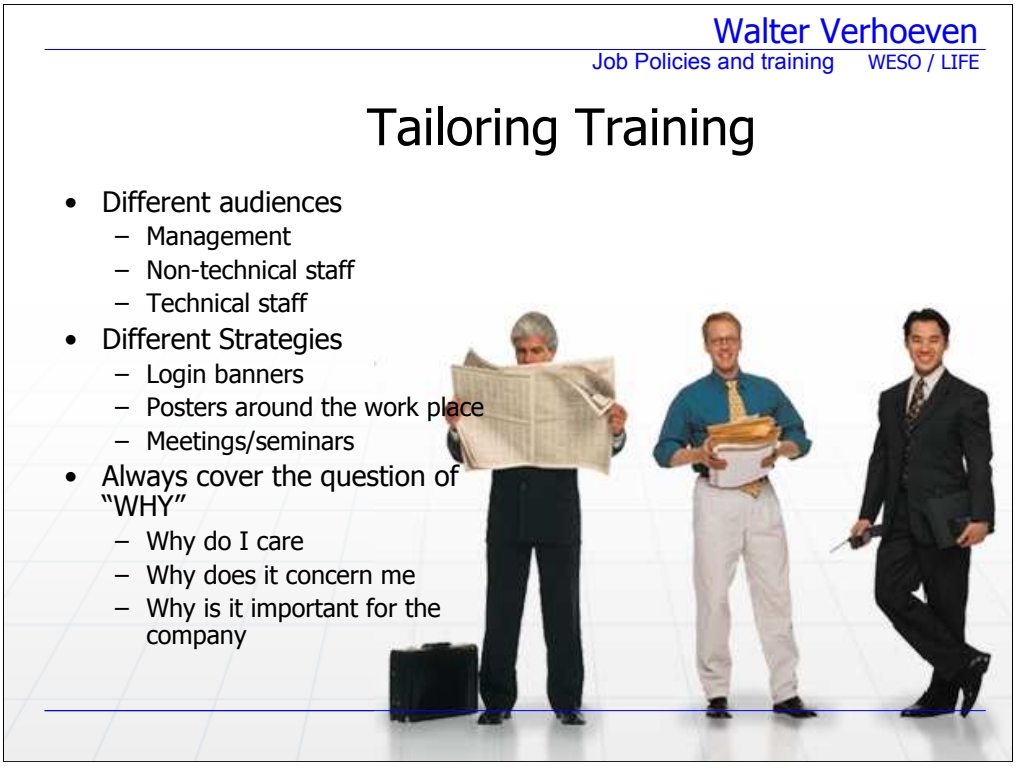
- Do all employees of the organisation and third party users (where relevant) receive appropriate information security training and regular updates in organisational policies and procedures.
- Are security requirements going to be addressed in the contract with the third parties when WESO outsources the management and control of all or some of its information systems, networks and/ or desktop environments.

  The contract should address:

  1. how the legal requirements are going to be met
  2. how the security of the organisation's assets are maintained and tested
  3. the right of audit
  4. physical security issues
  5. how the availability of the services is to be maintained in the event of disaster.

Training

- Who will provide awareness training?
- Some countries require a designated responsible individual to be a member of staff (Germany: Datenschutzbeauftragter).
- What training will be provided by outside specialists?
- How often will training seminars be held?

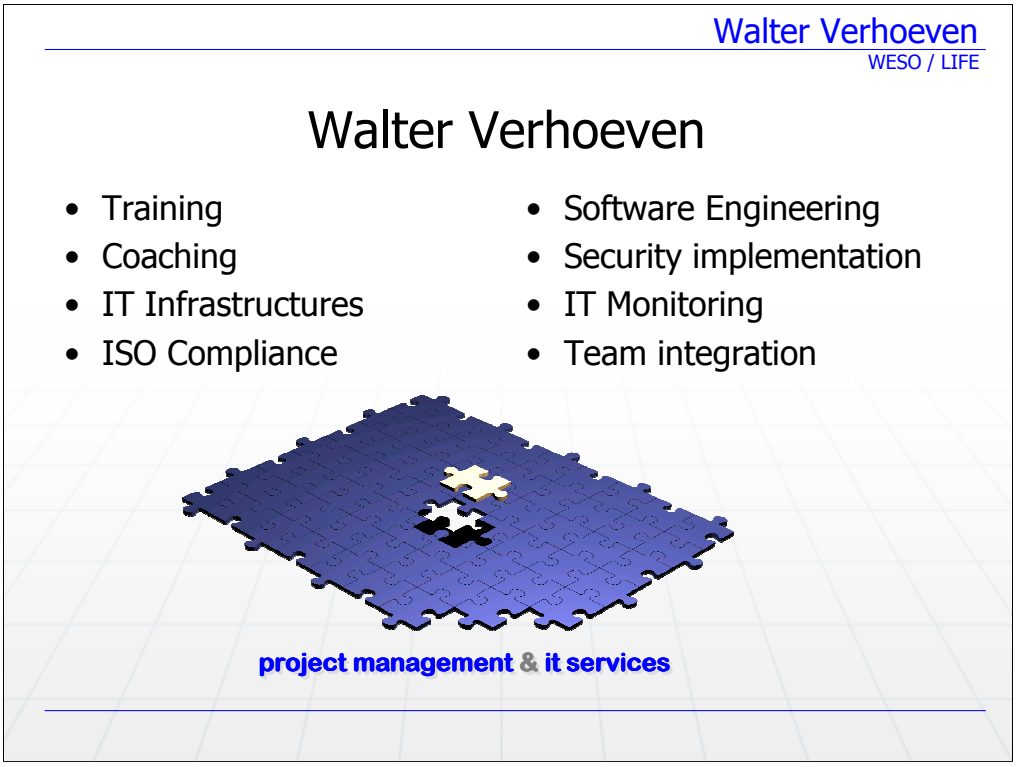


Management should be trained in analyzing the security reports as well as undergo training to stay in touch with the latest security issues as well as controls so that I can provide the best cost/value.

Technical staff needs to know what to do when a threat materializes. Training on how to manage infected computers.

Non-Technical staff needs to know whom to inform and what to do until help arrives (§6.3.1, §6.3.2, §6.2.2 of the ISO 17799 guidelines)

If the users do not understand why, they will not support or appreciate the security measures.



Thank you and we hope to have informed you.