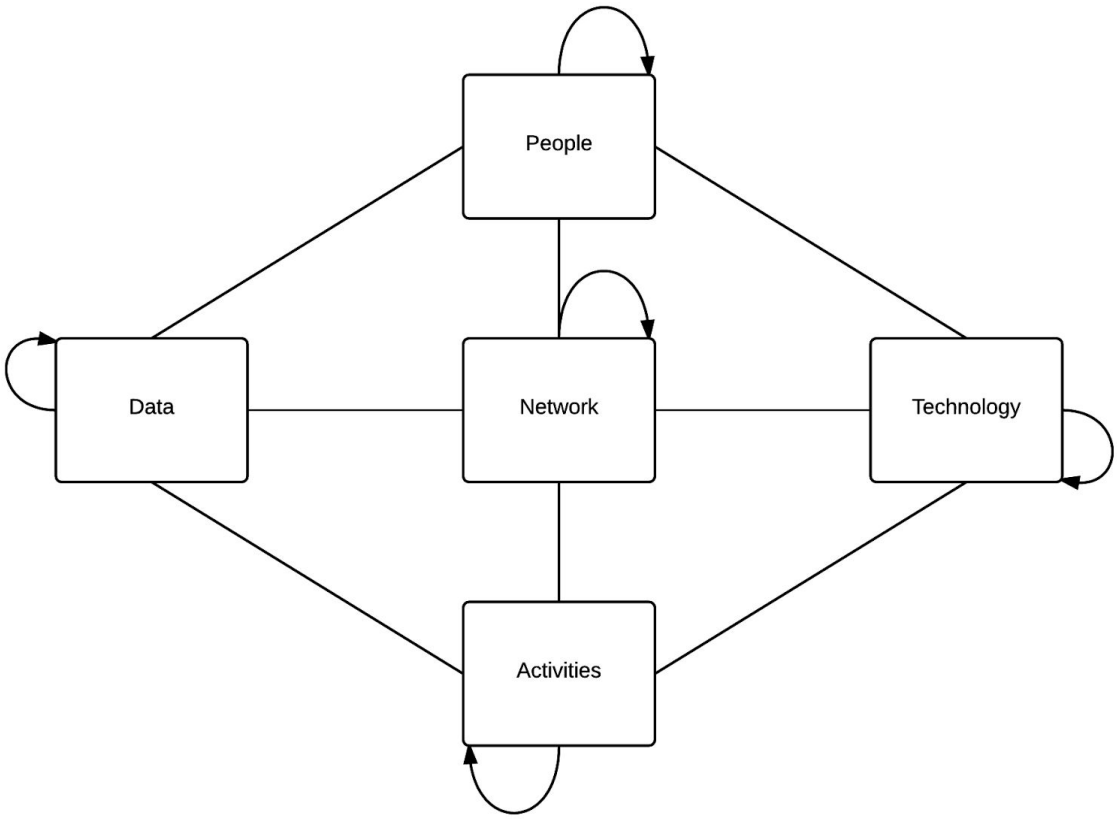
The role of Information Security

What are the different areas of information security in organizations?



What is the role of information security in an organization?

- Control of Information.
  - to protect valuable information and information systems
  - Theft, leakage, corruption, availability...
- CIA, non-repudiation, authentication (vs. authorisation)
  - The CIA triad of **confidentiality**, **integrity**, and **availability** is at the heart of information security.[12]
- To guarantee business continuity
  - Continuity of services and systems
- Risk management - risk driven
  - But also strongly compliance driven (e.g. legislation)

Is a separate information security function needed in an organization? Why or why not?

- Should be separate as central unit
    - answering directly on the CEO
    - Centralising the decision to be carried everywhere in the company
- Representative in each departement
    - Permit to not all focus on security but include it in each business units
    - Security need to part of the business, not on the side.

Who should be responsible over information security in an organization? How should this show up in the organization and its operations?

- Everybody
- CEO leading the way with the top management
    - Top management need to be knowledgeable in ISS
    - Support and enforce ISS

Define Risk, Vulnerability and Threat.

Risk is the likelihood that something bad will happen that causes harm to an informational asset (or the loss of the asset). A **vulnerability** is a weakness that could be used to endanger or cause harm to an informational asset. A **threat** is 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.

What are the key elements of a risk, i.e., what characteristics of a risk should be taken into account when it is evaluated (rated) & Evaluation of Security Risk

When a threat does use a vulnerability to inflict harm, it has an impact. In the context of information security, the impact is a loss of availability, integrity, and confidentiality, and possibly other losses (lost income, loss of life, loss of real property). It should be pointed out that it is not possible to identify all risks, nor is it possible to eliminate all risk. The remaining risk is called "residual risk".

Information security training

Put forward some basic principles regarding an efficient information security training session

- tailored by department
- apply directly to the work done by the user
- Practical case, not too long description
- Easy to use, understand documentation
- Make the user understand it's part of their work, and what they signed for, not an addon.

What are the challenges in developing efficient, yet practical, information security training in a large organization?

Creating a Information Security Culture.

- The security need to be part of the company culture
- Shared amongst all employees

Keep it simple is the biggest challenge. If the process explained is too complex, it won't be remembered and mistakes will happen.

Why do we have instructions ?

1. For compliance
    a. with standard
    b. organisation rules
2. For legal compliance
    a. with the law
3. Because others have them
    a. then you need it
4. Because our directors want to have them
    a. they knows what they're doing (or they should)
5. To describe secure behaviour
    a. Best way to teach

Responding to business disruptions: Raggad's 4 classes of safeguards

1. Deterrence safeguard
    a. Teach the disruptive agent the consequence of committing crime against the company.
    b. Publishing previous action done against "criminals"
    c. Based on the assumption that punishing an individual for a crime will deter other to commit the same crime.
    d. can be physical, sign, Software or Hardware
2. Detective safeguard
    a. Detecting a threat before it happens is the best way to avoid it to happen
    b. When detected early, it's easier to recover from the consequence

    c. Collecting information on the attacker, the attack, the progress of it and the impact are the first action to be taken
    d. Plan the response and initiate the plan + recovery procedure
3. Preventive safeguard
    a. Prevent instead of healing
    b. Prevent in area where risk is not accepted
    c. Already takes place in HR when hiring
    d. Contains fire security, insurance, etc ...
4. Corrective safeguard
    a. To activate the safeguard you need:
        i. Information about the current attack
        ii. Business component attacked
        iii. damages caused to them
    b. Activation
        i. Rank business by criticality
        ii. Then by damage extent
        iii. Identify alternative corrective action
        iv. Select the most feasible alternative
        v. Apply the alternative to the affected business

Tax Auditor Scenario

Method

The application of common knowledge and understand of the vulnerabilities in information system and society in general. (Common Sense)

Scenario

A tax auditor visits a customer company. When leaving the company he takes with him a large body of original papers concerning the customer's economical situation. In addition he uses his unencrypted USB memory token to copy confidential data from the customer's file server. This data will be analyzed in the auditor's own laptop, which will also be connected to his employer 's local area network.

On his way back to work, he stops to have some lunch. During the lunch the car is parked in a public garage the restaurant. All the papers, the USB token and the laptop are on the front seat of the car.

After the lunch he drives to work and connects his laptop into his employer's local area network. Next, he sticks his USB token into his laptop and copies the customer's data into his laptop's unencrypted hard drive an after that also into a file server's folder that is readable by all employees.

After work the auditor takes his laptop with him for remote working. At home, his kids want to play a new computer game. Thus, they connect their dad's laptop to the Internet and download and install a new game and start to enjoy playing.

Find and evaluate 5-10 obvious information security risks. Explain the method you use for evaluation.!

Risks

Leak of information. The tax auditor should have a secure access to his office from the client using a vpn. He will then access the data of the client on-site and analyse them on-site while putting his analysis in his virtual desktop hosted in his tax auditing company without the data ever being copied from the client server. A special access machine is provided for the tax auditor with logged access.

Stealing of Information. Using an unencrypted usb key that can be easily stolen and used directly is a major risk. In the case of using an USB key, it need to be encrypted and self destroyable in the case of wrong encryption key used especially if the data it contain are vital.

Loss of document. Since the original are taken they can be easily destroyed and lost forever. To avoid the risk, don't let the original leave the company and always keep backup.

Virus present on the usb key spreading in the network. There is no verification done before the tax auditor put his usb key in the client company computer. The key need to be scanned in a sandbox or in any other machine that is not connected to the network neither contain invaluable information.

Usb get tempered when left unattended. A hacker could get access to the usb key that is in the car and temper with the data while leaving a virus that will be installed in the tax auditing company. The USB need to stay with the Tax auditor and not leave him. He shouldn't do any stop with his car until he reach a safe location.

Corruption of data/destruction of data. When the work's computer is used for something else that what it meant to be. The tax auditor shouldn't let anybody use his computer for any non-related work

Training Plan

Short Info

Consider USB key as an unsafe method to transport client documents. The client data are vital for them, it should be the same for you.

Training Session

Requirements

1. IS security awareness training should take the learner's previous knowledge into account.
2. IS security awareness training should take possibilities and constraints caused by the instructional task, the learning environment, and the organizational setting into account.

3. IS security awareness training should enable systematic cognitive processing of information.
4. IS security awareness training should motivate for systematic cognitive processing of information.

Goals

- The goal was to use the learners' own authentic documents.
    - This aimed to make the instruction personally relevant to the learners' and in this way to motivate their cognitive processing.
- The learner's first task was to analyze their documents and find valuable, sensitive information in them.
- The next task was to analyze possible consequences to the company, to the team, and to the learners themselves if such information was revealed, e.g., to competitors.
    - The goal was to make the subject matter significant to the self and others.
        - This aimed to motivate learners' cognitive processing.
    - Another purpose of the task was to emphasize cause-and-effect.

What are the different sources of information security requirements in an organization?

- laws
- business, business areas
- authorities
- customers, other stakeholders
- everything else

However, impossible to meet all requirements (why ?)-