Information Security at the IEA – DPC

IEA General Assembly
October 10 – 12, 2011
Malahide, Ireland
General remarks

Impossible to cover all aspects of information security in a short presentation

Only sketch of main principles and activities to protect information

Focus will be on electronically stored and transmitted information

Many norms and standards are available that structure the field, e.g. published by the International Organization for Standardization (ISO)
Information

- Information can exist in many forms
  - Printed or written on paper
  - Stored electronically
  - Transmitted by post
  - Transmitted by electronic means

- Whatever form it takes, or means by which it is shared: It should always be appropriately protected
- Because: Information is the asset of the organization
Information security means

- protecting information and information systems from unauthorized activities.
- Wide range of activities is involved: access, use, disclosure, disruption, modification, perusal, inspection, recording, and destruction
Confidentiality

- No disclosure of information to unauthorized individuals or systems
- Legal or contractual reasons, policy of an organization

Integrity

- Data cannot be modified undetectably (neither in processing nor in transmission)

Availability

- Computing systems used to store and process the information, security controls used to protect it, and the communication channels used to access it must be functioning correctly
Evaluation of Risks and Countermeasures

What are vulnerabilities and threats to the information resources used by the organization?

- Items, source code of computer programs, technology, but also printing of test booklets, their storage...

What countermeasures, if any, need to be taken in reducing risk to an acceptable level, based on the value of the information resource to the organization?

Ongoing process of evaluation because the environment is changing constantly

- Internet, USB, mobile devices
Choice of countermeasures (controls) used to manage risks must strike a balance between productivity, cost, effectiveness of the countermeasure, and the value of the informational asset being protected.

Possible to implement almost secure procedures and technology, but extremely costly and working procedures will be blocked in an unacceptable way.

- **Technical level**
  - Backups, access limitations, logging

- **Organizational level**
  - User groups

- **Personal level**
  - Training, raising of awareness, confidentiality agreements,
Implementation at the IEA – DPC

Keep in mind: mission of the organization and the type of data

Trend data for international comparisons

Highly anonymized --> re-identification of individuals is almost impossible

Data are collected to be published

All data are available in the internet

Complete documentation and reports are provided

Auxiliary programs can be downloaded for free
General Security Measures

- Alarm system
  - Each room and window is equipped with at least one detector
  - Burglary, assault directly reported to security and police

- Fire and smoke detection
  - Directly reported to fire department
Access Control

Entrance control to IEA – DPC premises
- Photo ID for all employees
- Visitor ID cards
- Separate conference rooms for training, seminars, workshops... (no permanently network connected computers)
Access Control (ctd.)

- User log in and password required to access the network
- Access to data ruled by well defined user groups
  - Project specific
    - Contractual requirement: Confidentiality agreements at project level
  - Task specific
    - Access to source code by software unit only
- Depending on sensitivity of data and necessity to work with the data
- Examples
  - Data coming from countries
  - Instruments
  - Items under embargo
  - Draft reports
Data Transmission

- Secure FTP is used to exchange data with partners
- Firewalled system with two firewalls
  - Internal-external
  - Linux based (less vulnerable because Microsoft products are in the focus of attacks)
- Policy: deny-all
- Problem: tunneling of services (skype etc., Teamviewer etc., emule etc., iTunes player)
- No email transfer of sensitive data
- Data encryption techniques for temporary storage on laptops
- No download of unauthorized software
Protection Against Malware

- Malicious software that can take a variety of forms of hostile, intrusive, or annoying software or program code
- Computer virus, computer worm, trojan horse/trojan, spyware/adware, keylogger....and spam
- Anti – virus software
Rejection of Mail

Mailserver

filtering (FProt, SpamAssassin)

more than 1 million rejected mails!
Personalized Data

- New challenge in longitudinal studies; students need to be approached directly by mail
- Storage of names and addresses
- High requirements from data protection authorities with respect to storage, transmission, duration of storage, erasure, logging...
- Information is stored in a separate network
  - No USB, no email, no internet
- Exchange via SQL server that can be operated with highest admin rights only
- Two computers under the table of selected staff members
- Staff can switch keyboard and screen, but has no chance to connect both worlds
Closed network
Storage

- Redundant data storage system (RAID System)
- Battery backup against power failure
- Daily backup of crucial data
- External storage of backup tapes
- Recovery time < 24 hrs
Integrity of Processes

- All changes to data are monitored and recorded
  - Program runs are logged
  - Person in charge can be identified

- Manual changes are logged
  - Identification of the operator
  - Time of action
  - Type of change
  - Reason for change
Challenges in the future

- **Mobile devices**
  - Smart phones, tablet computers, iPad...
  - If not provided by IT they are an area out of control and a perfect gate for malware into the system
  - Access to mail with private phones is prohibited

- **Remote access**
  - So far prohibited
  - Review of necessity, risks, types of data, user groups...
  - Authentication
  - Costs (not only for acquisition, but also for implementation, maintenance, changes in procedures, training, etc.)
Thank you!