cphbusiness

IT-Security

- Organizational view

Wind of changes

- Two hundred years ago, you probably would have made a living in agriculture.
- One hundred years ago, you most likely would have worked in a factory.
- Today, we live in the Information Age and almost everyone has a job somehow connected to information stored in digital form on a network.

Important ?

- During the agricultural age, crops and the tools to produce them were the most important asset.
- During the industrial age, manufactured goods and the factories that produced them were the most important asset.
- Today, information is a key asset of almost every organization and individual!

Stealing and spying

- Once spying was person against person, country against country.
- Today, spies sit on fiber-optic cables and our wi-fi networks.
- They steal data and information without breaking any glass.
- Keeping data confidential is one core mission of information security (think identity theft!)

Right or Wrong

- Wrong information is worse than no information.
- When users of information lose confidence that the information is accurate, they'll never rely on it.
- Everybody who tried to fix an inaccurate credit report know that's not easy!
- Maintaining data integrity is also a core mission of information security.

Easy security – lock down!

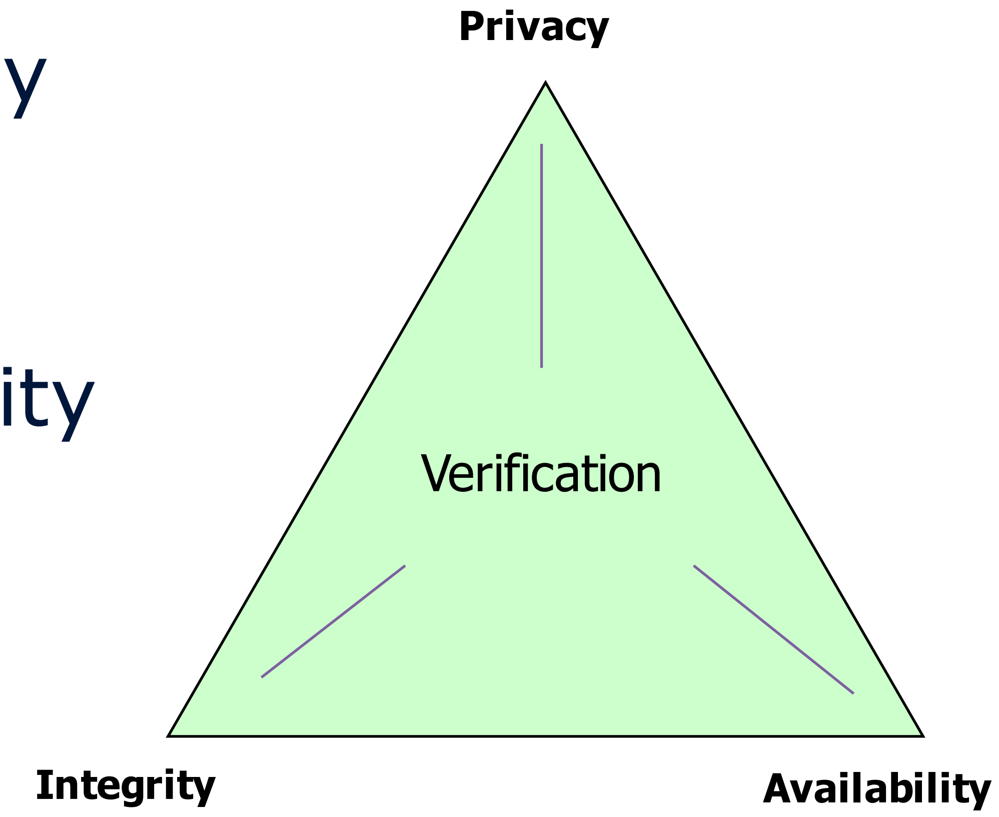
- Information security doesn’t mean locking everything down.
- If people don’t have the information they need, they can’t do their jobs.
- Information security professionals must be able to balance access to information and the risk of damage.
- A third core mission of Information Security is making information available when needed.

The 3 core missions of Information Security:

- Making information available when needed.
- Keeping data confidential
- Maintaining data integrity

Security Objectives

- Confidentiality / Privacy
- Integrity / credibility
- Availability /accessability
- Verification of identity



IT Security - New Challenges!

- The requirements for our IT security is increasing day by day. On the one hand, they handle the growing need for remote access to our IT systems to partners, home offices and traveling employees – access increasingly using wireless communication. And on the other, they effectively protect against internal and external attacks that become more frequent and more sophisticated.
- Telecommuting has become substantially more attractive with the new broadband services by which we communicate quickly and cheaply via the Internet, but also expose our IP address, which provides new opportunities for attack. It is therefore vital that the creation is done in a way that does not expose domestic work and in particular its core systems for safety hazards.
- The possibilities of using wireless communications have been infinite, and new technologies and services emerge every day - both for remote communication and for our internal communications within the company or home.

Need for transparency and communication are greater than ever - so is the need for security!

Elements of security

- Prevention
  - Firewalls, authentication, segmentation, antivirus etc.
- Discovery
  - Intrusion Detection, log analysis, alerting, etc.
- Repair
  - Backup systems, insurance, containment, etc.

- Risk = Probability x impact

Risks & threats

- Viruses and Trojans
  - E-mail viruses, macro viruses, worms
- Discrediting
  - Deface by a web server, mail spoffing
- Denial of service
  - DoS, Unable to work / use computer systems
- Loss of data
  - Data is lost when the systems are destroyed, downtime
- Compromise of data
  - Breach of confidentiality / secrecy, modification of data
- Unauthorized access
  - Springboard - can be used to compromise other web servers
  - Distribution of illegal / pirated material

”It’s not a bug - it’s a feature!”

- Millions of people searching for unsecured systems and will love to damage them

Risk Reduction

- Risks can not be removed, only limited
- Security can not be purchased as a product
- Security is achieved by a combination of
  - Procedures & Management / (management issues)
  - Design, tools and technical solutions
  - Ongoing monitoring and maintenance

Result: Formulation of security policy and implementation of safety system