BSI Baseline Protection Manual
- How to measure IT-Security -

Thomas Biere
Bundesamt für Sicherheit in der Informationstechnik
Federal Information Security Agency, Germany

Prejudices against IT-Security

- IT-Security
  - causes a lot of expenses
  - is too expencive
  - hinders the users to do their jobs
  - causes much more work in the IT-administration
  - is only something for larger companies

IT-Security

Why should I think

about

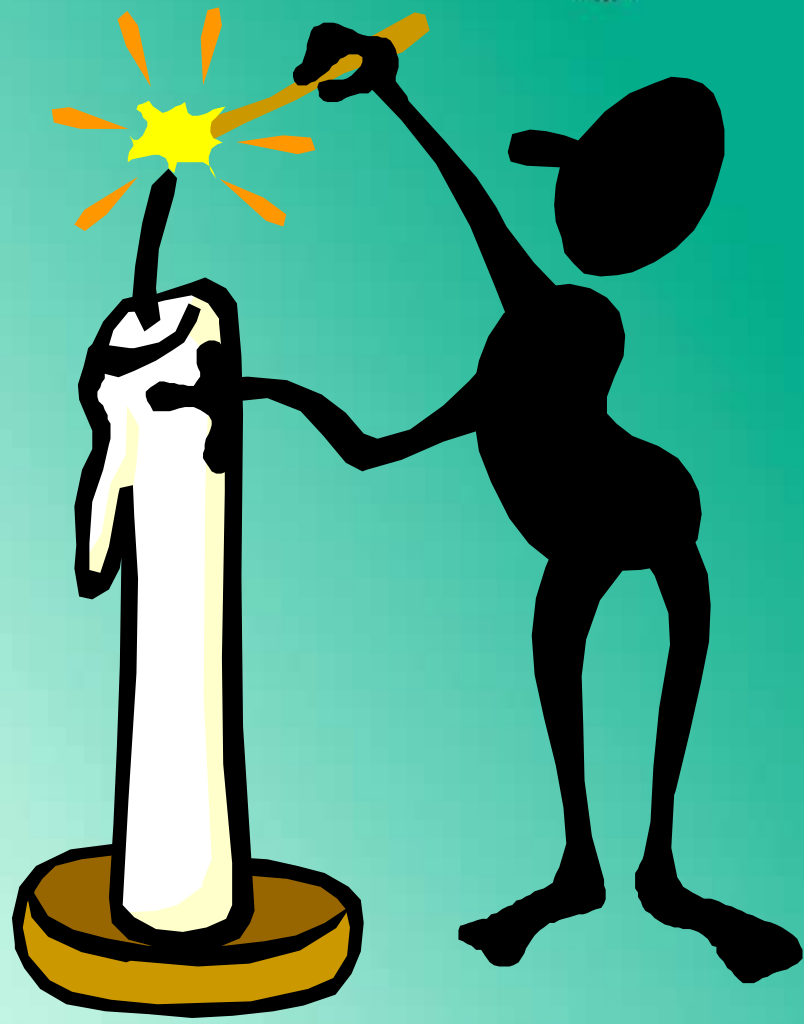
IT-Security?

The importance of IT

- nearly all companies are using IT
- nearly all processes depend on IT
- the niveau of local and global networking rises up
- the IT becomes more and more complex
- the systems has been opened (remote access, internet)

The importance of IT

rising up dependency
means
opening for attacks



In IT-Security interested people and organisations

internal:

- the board
- the owner
- the IT-security-management
- the internal audit management
- the marketing

external:

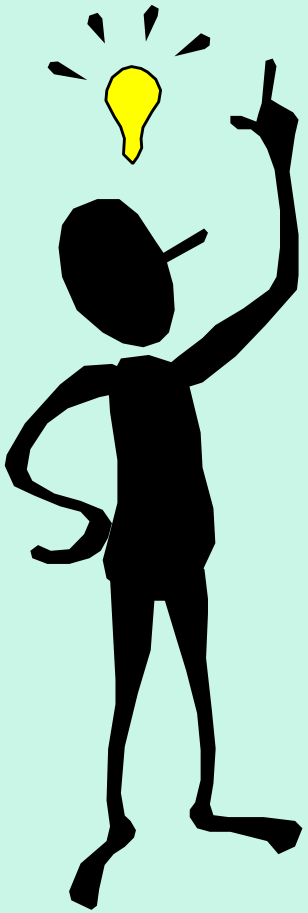
- customers
- business partners
- the banks
- insurers
- authorities
- courts of justice
- the prosecuting attorney's office

Internal measurability

problems:

- no possibility to make balance between the pros and cons
- there are no parameters of business management
  - the return of investment is not measurable
- some categories of use and damage are not scalable
- paradoxon of security: people see the necessity to invest in IT-Security only, if something happens

Internal measurability



- to measure the effectiveness of IT-Security by registering of incidents
  - you need a special organisation to be able to register all incidents
  - you need the results of registering from some years
  - it is not very useful, if a seldom but catastrophic event happens
  - it is not useful to document externally the level of IT-Security

Demands

Demands

- state of IT-Security
  - it should say something about the state of IT-Security of a IT-combine and the IT-Security management
- completeness
  - all parts of an IT environment should be objects of the survey
- lucidity
  - the results must be lucid

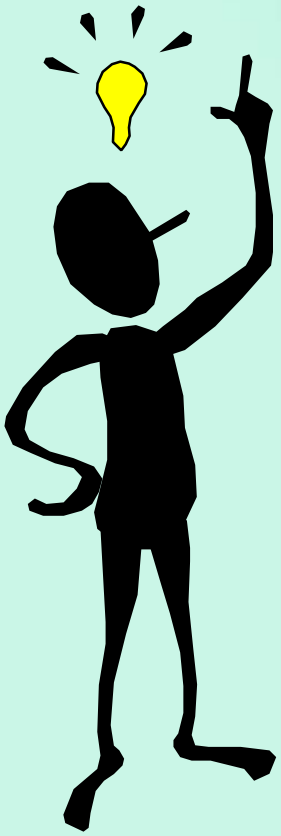
Demands

- comparability
  - the results must be comparable
- methodology of the survey
  - the methodology of the survey must be exactly defined
- relevance
  - the results must be relevant
- documentation
  - one of the results of the survey should be a documentation

Demands

- expenses
  - the expenses for the process should be low
- benchmarking
  - there must be the possibility to compare the own company with other companies. The aim: increasing the level of IT-Security
- publication
  - the marketing should be able to use the results of the process

IT-Security



We have something like a standard for

IT-Security:

The BSI Baseline Protection Manual

IT Baseline Protection

Main ideas

- The whole system consists of typical components (e.g. server and client computers, operating systems)
- Threats and their probabilities are lumped together.
- Suitable groups of Standard Security Safeguards are recommended.
- Detailed pieces of advice for the implementation of these safeguards are included.

IT Baseline Protection

Advantages

- A simple target/performance comparison allows for economic application and procedures.
- Resulting IT security concepts are compact due to references to standard source.
- Practical, reliable, and effective safeguards are implemented.
- The concept is expandable and continuously updated.

IT Baseline Protection

The aim is

to achieve a security level for IT installations by appropriate employment of organisational, personnel, infrastructural, and technical

standard security measures

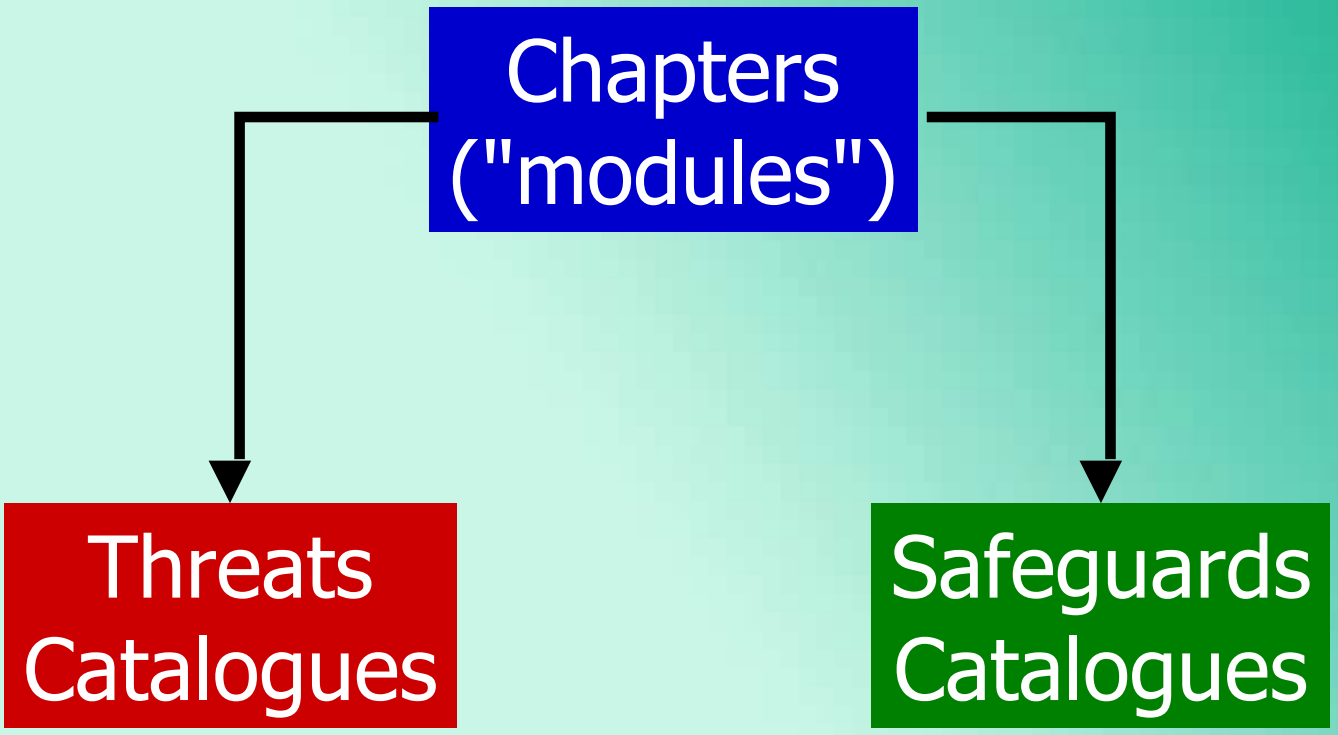
which is adequate and sufficient for

average protection requirements

and may also serve as a basis for IT applications with

higher protection requirements.

Structure of the IT Baseline Protection Manual



Structure of the IT Baseline Protection Manual

Modules (examples)

- Personnel
- Contingency Planning
- Data Media Archives
- Windows NT
- Unix-Server
- Lotus Notes
- Remote Access
- Mobile phone

About 50 modules on technical and non-technical aspects of IT security

Structure of the IT Baseline Protection Manual

Threats Catalogues and examples

- T 1 Force majeure
  - T 1.6 Burning cables
  - T 1.7 Inadmissible temperature and humidity
- T 2 Organisational Shortcomings
  - T 2.29 Software testing with production data
  - T 2.61 Unauthorised collection of personal data

Structure of the IT Baseline Protection Manual

Threats Catalogues and examples

- T 3 Human Failure

  T 3.25 Negligent deletion of objects

- T 4 Technical Failure

  T 4.16 Fax transmission errors

- T 5 Deliberate Acts

  T 5.88 Misuse of active contents

Structure of the IT Baseline Protection Manual

Safeguards Catalogues and examples

- S 1 Infrastructure

  S 1.21 Sufficient dimensioning of lines

- S 2 Organisation

  S 2.46 Appropriate key management

- S 3 Personnel

  S 3.17 Briefing personnel on modem usage

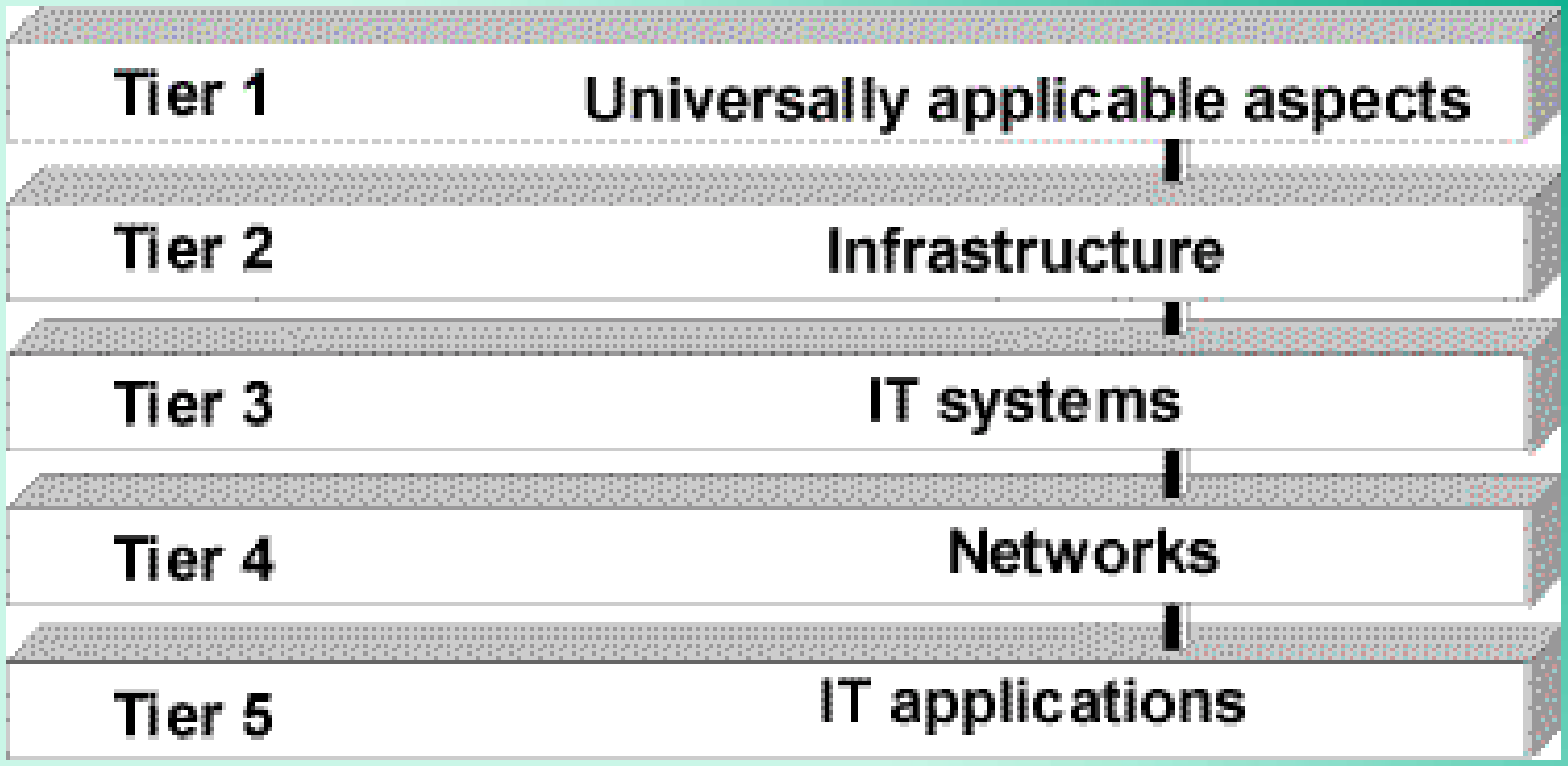
Structure of the IT Baseline Protection Manual

Safeguards Catalogues and examples

- S 4 Hardware/Software
  S 4.97 One service per server
- S 5 Communications
  S 5.45 Security of WWW browsers
- S 6 Contingency planning
  S 6.11 Development of a post-incident recovery plan

Structure of the IT Baseline Protection Manual

Modules



Structure of the IT Baseline Protection Manual

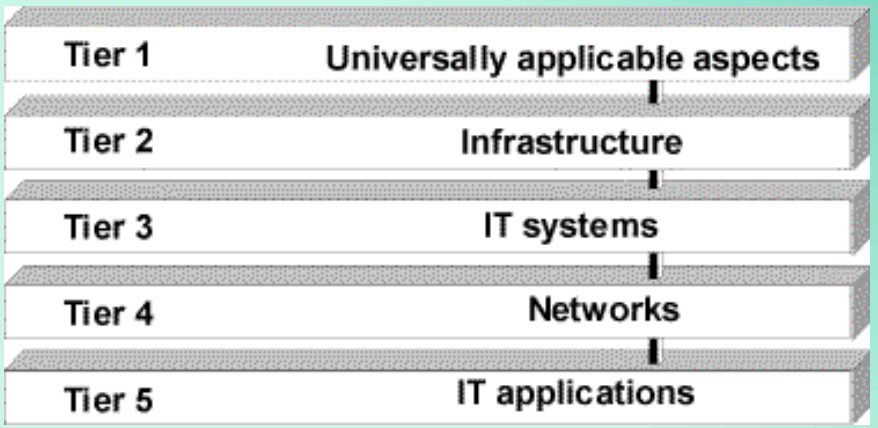
Modules

- Tier 1: general IT security aspects (e.g. IT Security Management, Organisation, Data Backup Policy and Computer Virus Protection Concept)
- Tier 2: infrastructural security (e.g. Buildings, Rooms, Protective Cabinets and Working Place at Home)
- Tier 3: IT systems (e.g. Unix System, Laptop, PC, Windows NT Network and Telecommunications System)

Structure of the IT Baseline Protection Manual

Modules

- Tier 4: networks (e.g. Heterogeneous Networks, Network and System Management and Firewalls)
- Tier 5: IT applications (e.g. E-Mail, WWW Server, Fax Servers and Databases)

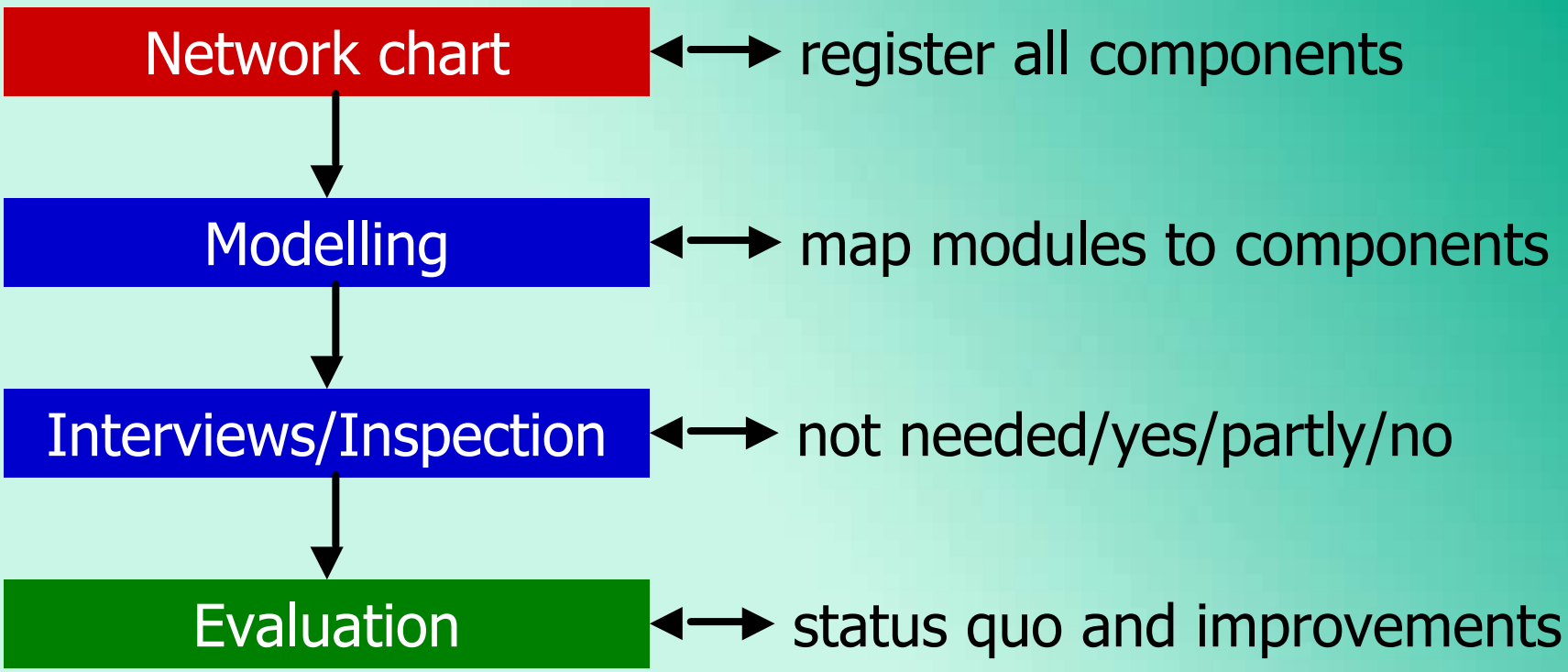


Structure of the IT Baseline Protection Manual

New modules

- IT security management (reorganised as a module)
- Remote Access
- Mobile phone
- Lotus Notes
- Computer centre
- Windows 2000 (March 2002)
- MS Internet Information Server (March 2002)
- Apache Web Server (March 2002)

How to apply the IT Baseline Protection Manual



Some facts about the IT Baseline Protection Manual

- about 4500 voluntarily registers users worldwide
- has become one of the de-facto standard reference manuals for IT security in Germany
- available as a printed loose-leaf edition (German only)
- available on CD-ROM (English and German)
- available on the Internet (English and German)
  http://www.bsi.bund.de/gshb
- a certification scheme will be available soon

Qualification according to IT Baseline Protection

Motivation

- Agencies and companies want to identify the security level of co-operating institutions.
- Institutions want to demonstrate, that they have successfully applied IT Baseline Protection.
- Companies want to make their efforts regarding IT security transparent to clients and customers.

Qualification according to IT Baseline Protection

Terms

- BSI is going to define a "Qualification Scheme according to IT Baseline Protection".
- Having completed this scheme the institution is awarded an "IT Baseline Protection Seal".
- Two entry-level seals and the final "IT Baseline Protection Certificate" will be offered.

Qualification according to IT Baseline Protection

Three different seals

- "IT Baseline Protection Certificate"
  granted by an accredited testing laboratory.
  All required safeguards are implemented.
- "Advanced Seal"
  Most important safeguards are implemented.
- "Entry-level Seal"
  The essential safeguards are implemented.

Any questions???