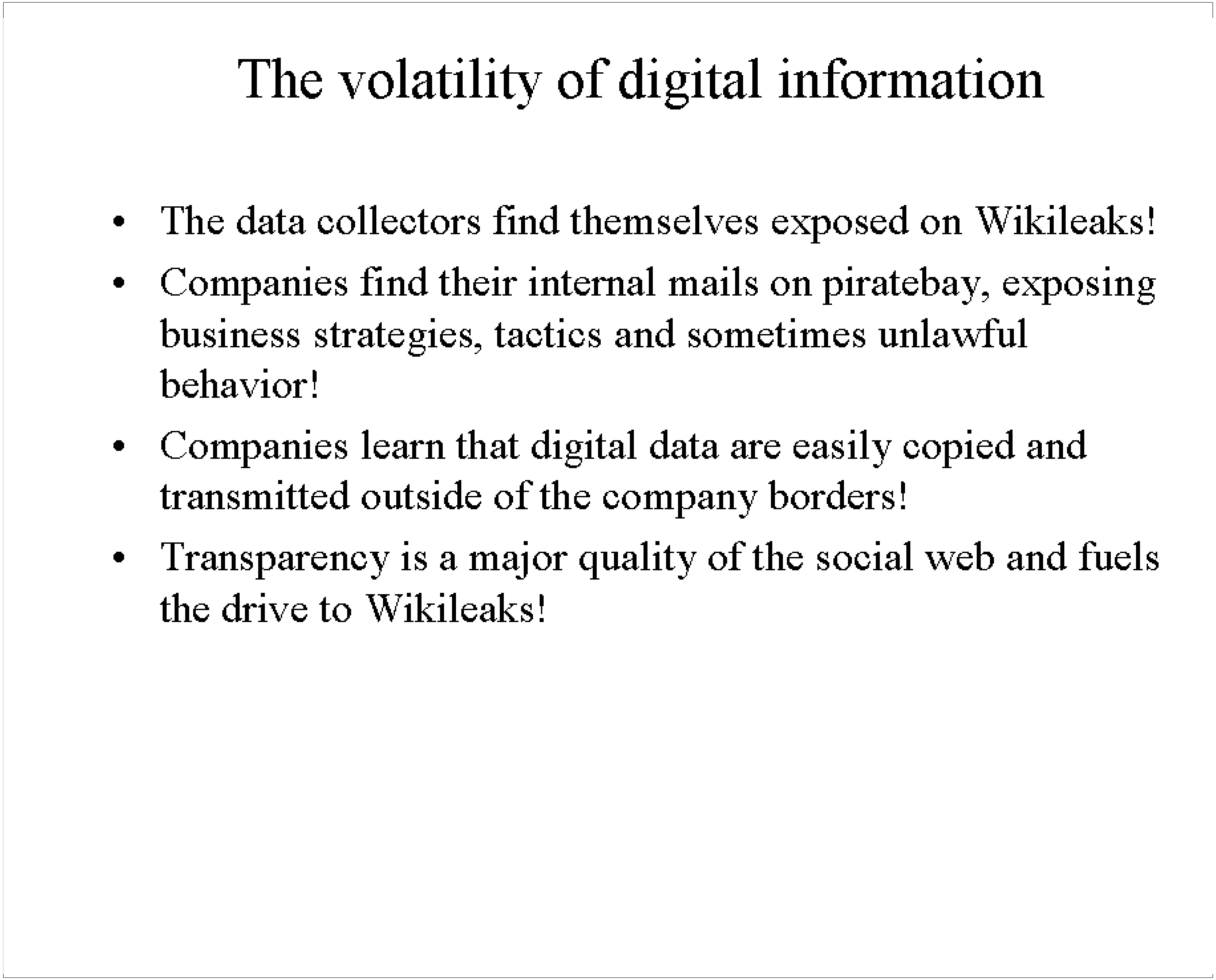
A conceptual framework for (not only) Corporate Security

Lecture on

Advanced Internet Security

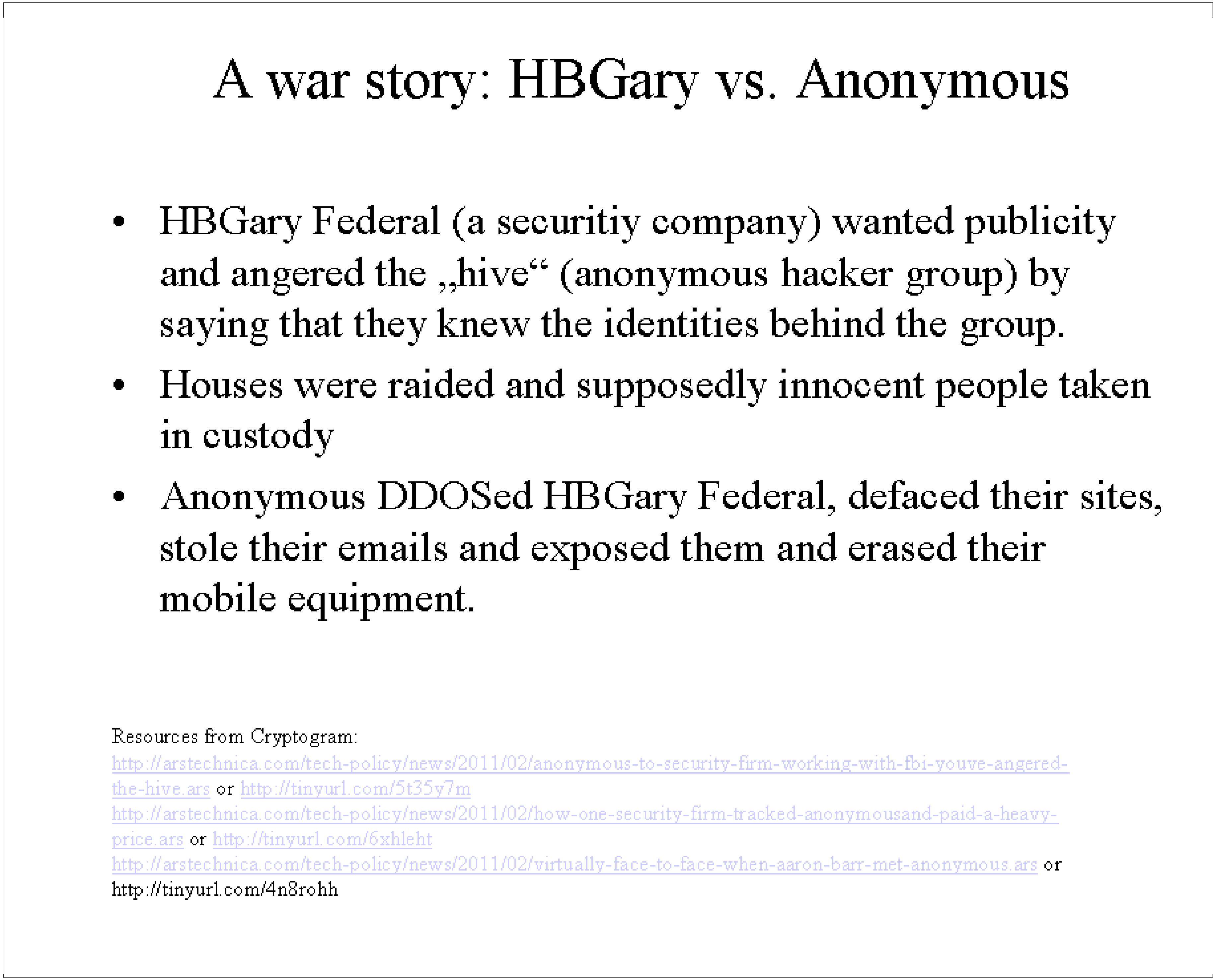
A framework for Security

Walter Kriha



The volatility of digital information

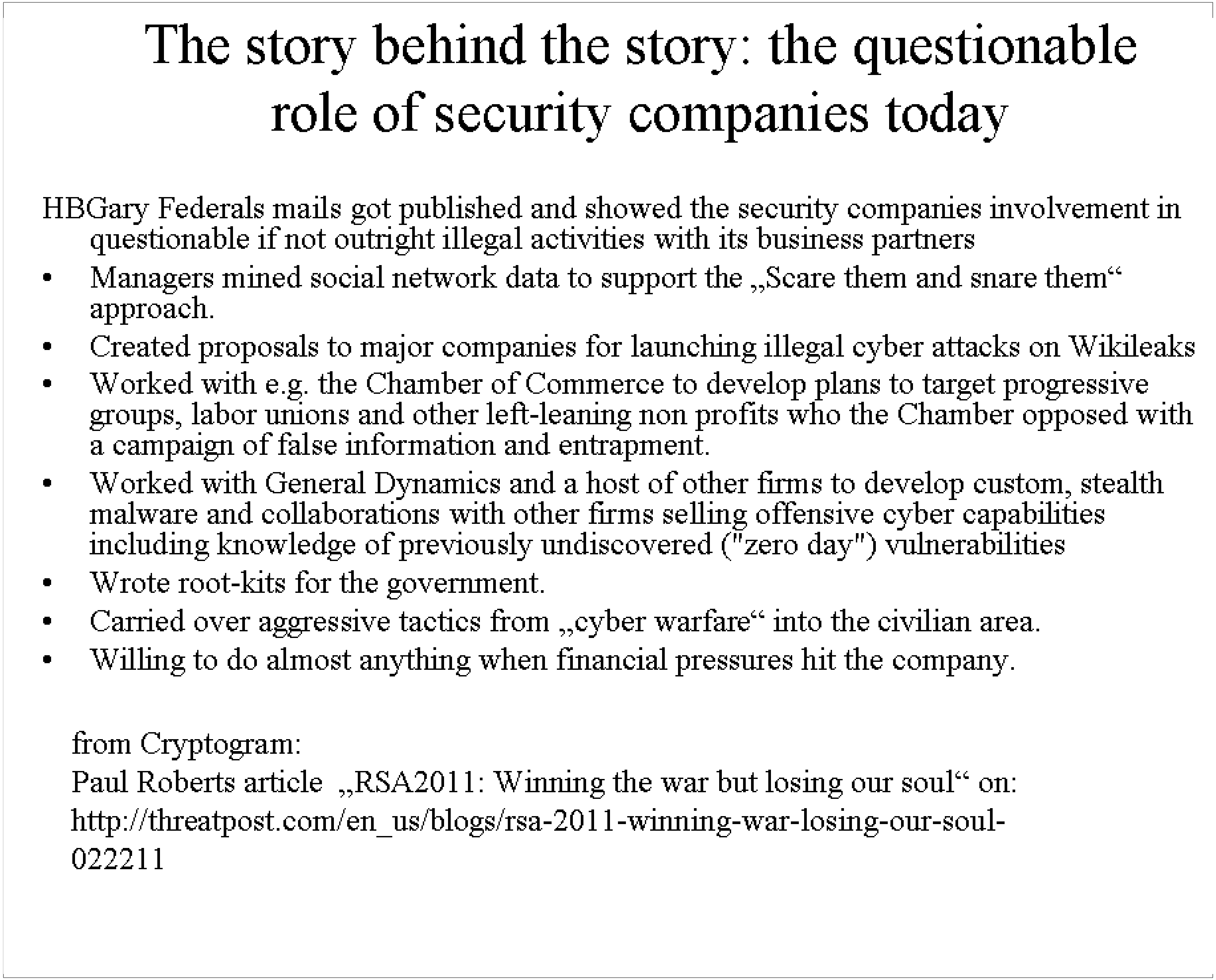
- The data collectors find themselves exposed on Wikileaks!
- Companies find their internal mails on piratebay, exposing business strategies, tactics and sometimes unlawful behavior!
- Companies learn that digital data are easily copied and transmitted outside of the company borders!
- Transparency is a major quality of the social web and fuels the drive to Wikileaks!



A war story: HBGary vs. Anonymous

- HBGary Federal (a securitiy company) wanted publicity and angered the „hive“ (anonymous hacker group) by saying that they knew the identities behind the group.
- Houses were raided and supposedly innocent people taken in custody
- Anonymous DDOSed HBGary Federal, defaced their sites, stole their emails and exposed them and erased their mobile equipment.

Resources from Cryptogram:
http://arstechnica.com/tech-policy/news/2011/02/anonymous-to-security-firm-working-with-fbi-youve-angered-the-hive.ars or http://tinyurl.com/5t35y7m
http://arstechnica.com/tech-policy/news/2011/02/how-one-security-firm-tracked-anonymousand-paid-a-heavy-price.ars or http://tinyurl.com/6xhleht
http://arstechnica.com/tech-policy/news/2011/02/virtually-face-to-face-when-aaron-barr-met-anonymous.ars or http://tinyurl.com/4n8rohh



The story behind the story: the questionable role of security companies today

HBGary Federals mails got published and showed the security companies involvement in questionable if not outright illegal activities with its business partners

- Managers mined social network data to support the „Scare them and snare them“ approach.
- Created proposals to major companies for launching illegal cyber attacks on Wikileaks
- Worked with e.g. the Chamber of Commerce to develop plans to target progressive groups, labor unions and other left-leaning non profits who the Chamber opposed with a campaign of false information and entrapment.
- Worked with General Dynamics and a host of other firms to develop custom, stealth malware and collaborations with other firms selling offensive cyber capabilities including knowledge of previously undiscovered ("zero day") vulnerabilities
- Wrote root-kits for the government.
- Carried over aggressive tactics from „cyber warfare“ into the civilian area.
- Willing to do almost anything when financial pressures hit the company.

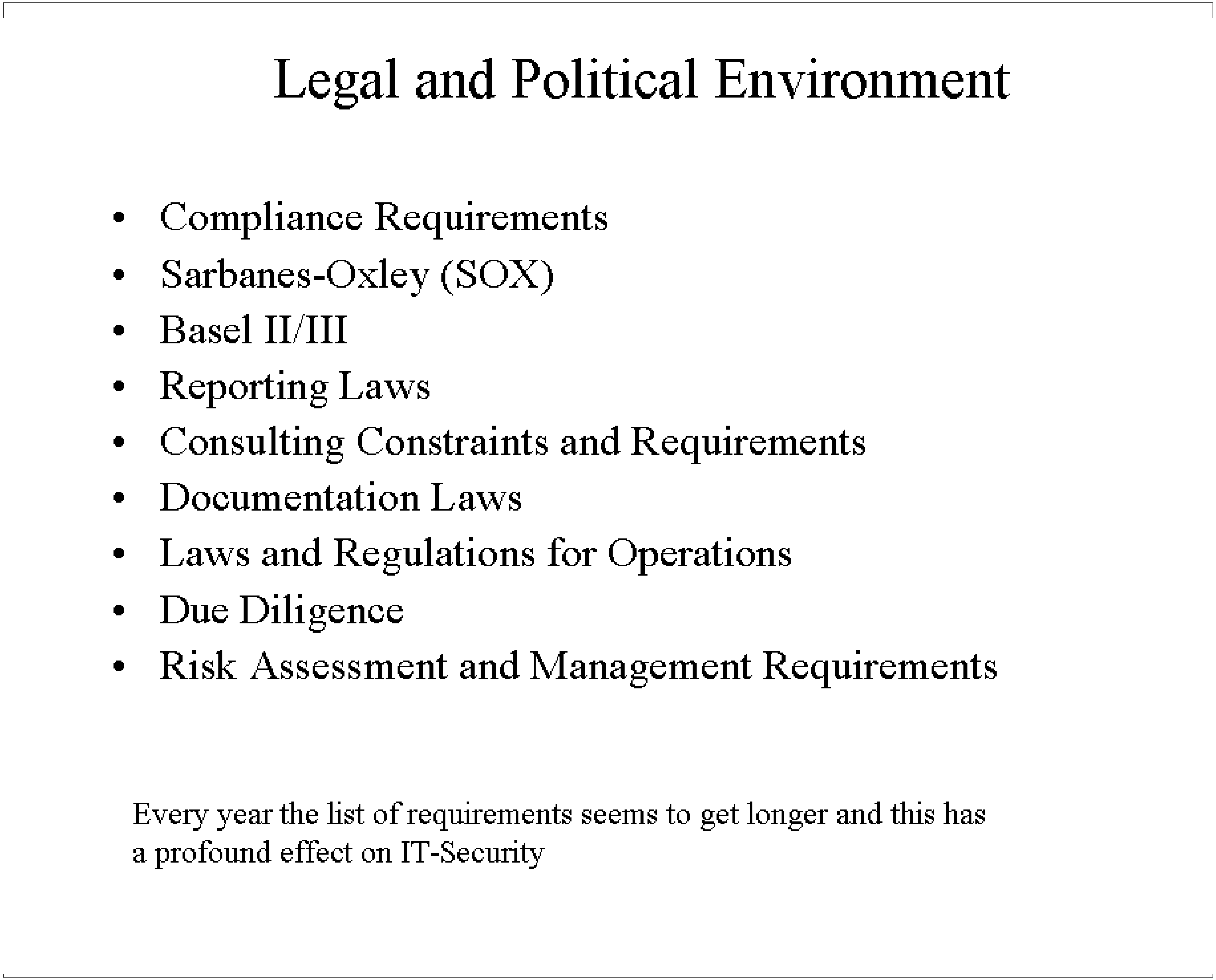
from Cryptogram:

Paul Roberts article „RSA2011: Winning the war but losing our soul“ on:

http://threatpost.com/en_us/blogs/rsa-2011-winning-war-losing-our-soul-022211

Threats

- Data Leaks
- Attacks on Universal Communication and Collaboration
- Identity Theft
- Social Engineering
- Mobility and Peer-to-Peer Attacks
- Information Attacks
- Malware Attacks
- Phishing, Pharming etc.
- DDOS Attacks
- Insider Attacks



Legal and Political Environment

- Compliance Requirements
- Sarbanes-Oxley (SOX)
- Basel II/III
- Reporting Laws
- Consulting Constraints and Requirements
- Documentation Laws
- Laws and Regulations for Operations
- Due Diligence
- Risk Assessment and Management Requirements

Every year the list of requirements seems to get longer and this has a profound effect on IT-Security

Corporate Security: Two important messages

- There is no clean separation between Internet and Intranet Security (de-perimeterization)
- Every security analysis or design needs a framework of rules and policies to compare with. A point of reference!

BTW: what where the two main messages from last week?

Goals

Define a framework for company security. It will be the base for all legal, financial, business and technical aspects of a company-wide security implementation.

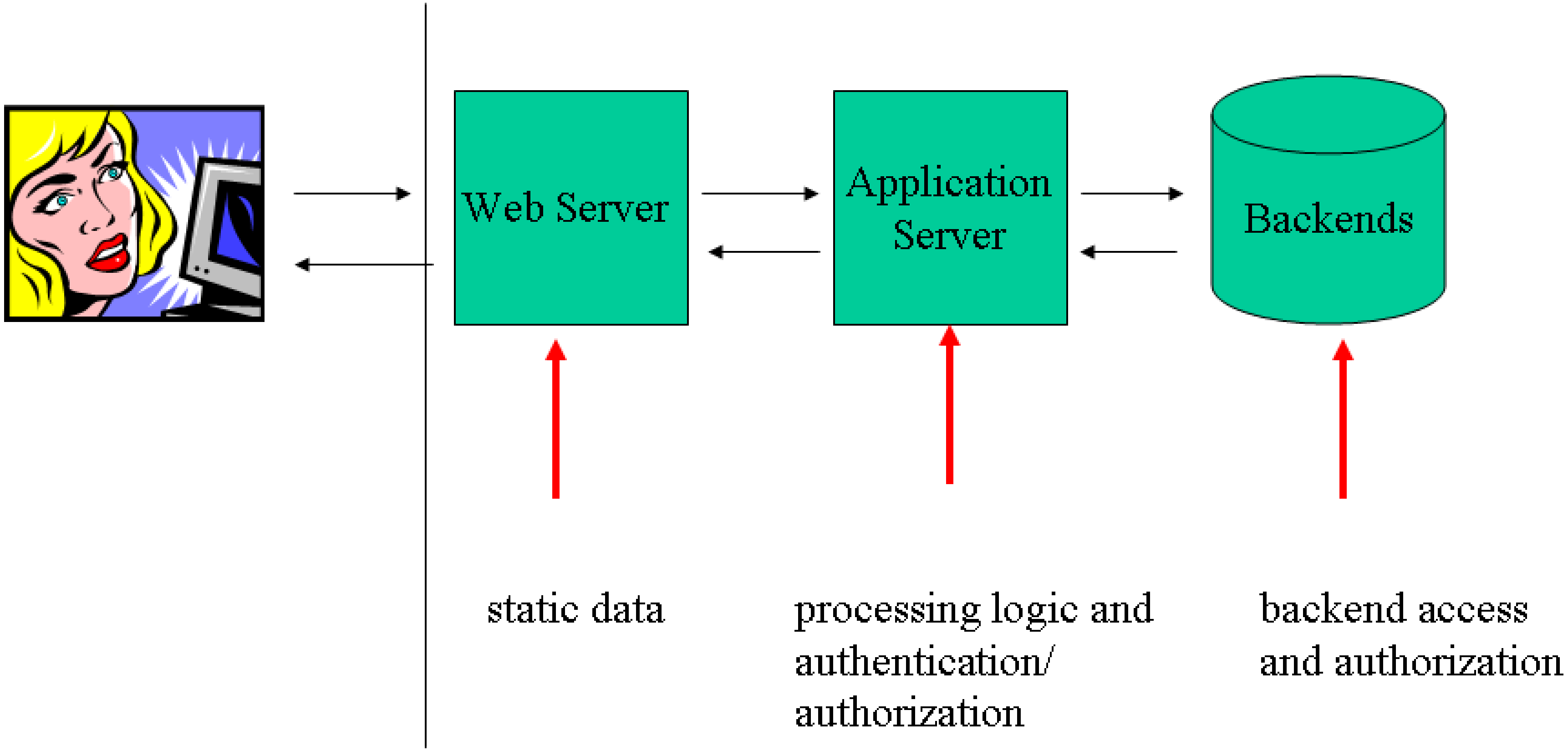
Define fundamental security statements from the policy

Show how concrete requirements, rules and directives are derived from the security framework.

Define a technical security architecture that implements mechanism and systems in compliance with the security policies and functions

Don‘t forget that security needs money and top level management support to work. The top down approach used here actually is the management pattern of continuous refinement from policy to implementation.

Internet Security?



Web Server

Application Server

Backends

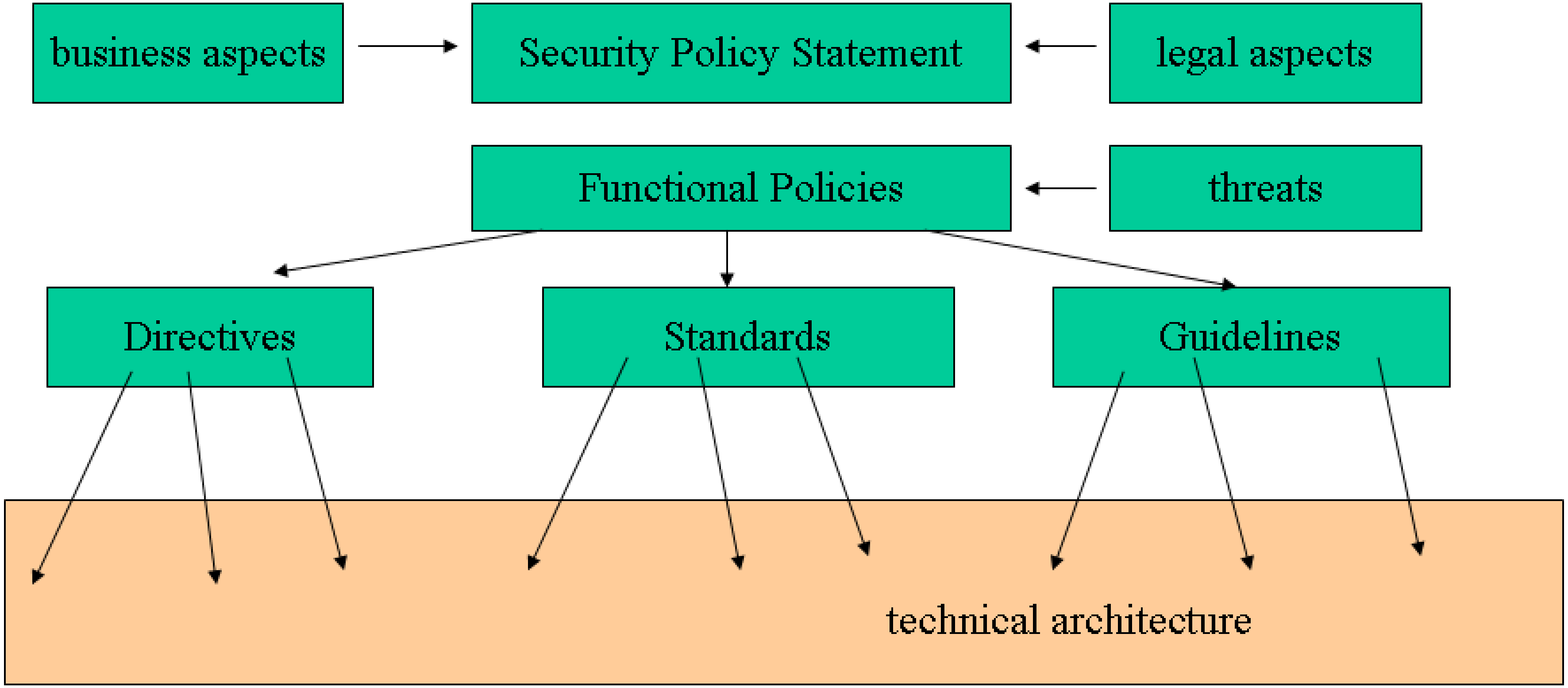
static data

processing logic and authentication/ authorization

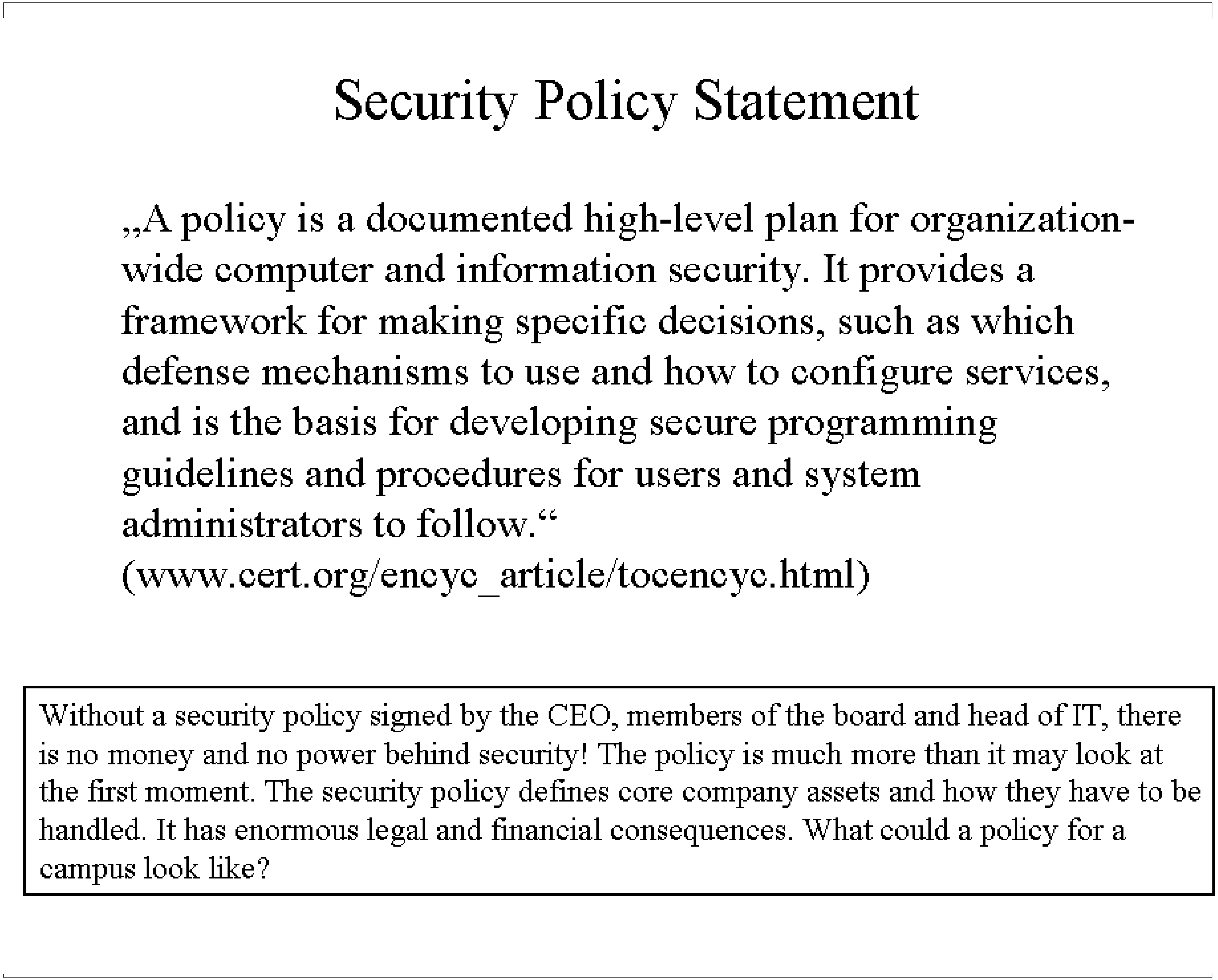
backend access and authorization

All of the information provided to the internet come usually from the intranet. This means that there is no real divide between both networks. Internet security therefore includes intranet security – otherwise data and functions can get exposed without permission. What is more dangerous? Incoming or outgoing traffic?

Part I: Security Framework



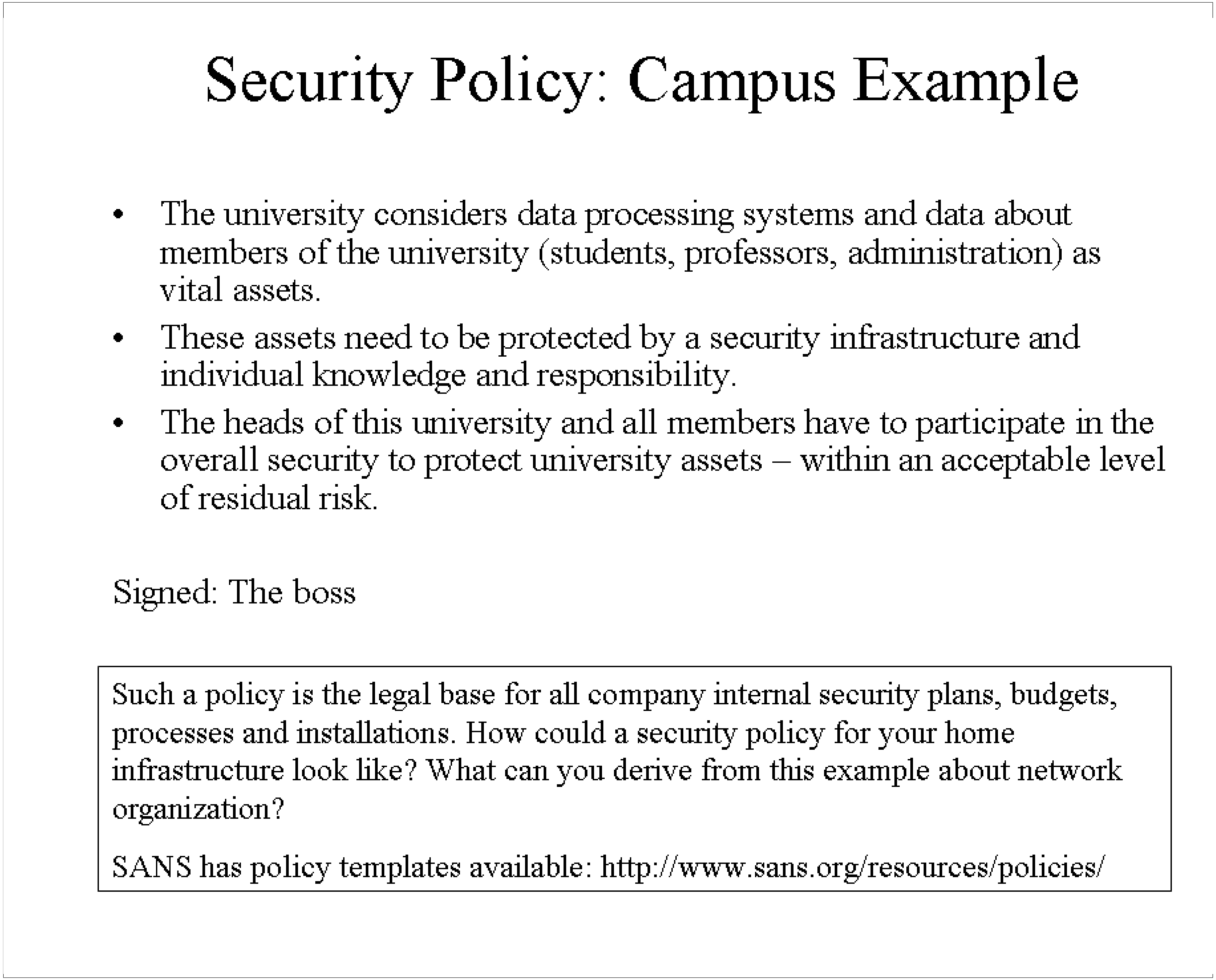
The security framework is the reference for all security related questions in a company. It defines risk management principles, responsibilites and last but not least the technical implementation e.g. of Internet security rules. The security policy is like a mission statement or a strategic vision. If you want to learn more about those things, attend an IBM Global Services Method Workshop.



Security Policy Statement

„A policy is a documented high-level plan for organization-wide computer and information security. It provides a framework for making specific decisions, such as which defense mechanisms to use and how to configure services, and is the basis for developing secure programming guidelines and procedures for users and system administrators to follow.“
(www.cert.org/encyc_article/tocencyc.html)

Without a security policy signed by the CEO, members of the board and head of IT, there is no money and no power behind security! The policy is much more than it may look at the first moment. The security policy defines core company assets and how they have to be handled. It has enormous legal and financial consequences. What could a policy for a campus look like?



Security Policy: Campus Example

- The university considers data processing systems and data about members of the university (students, professors, administration) as vital assets.
- These assets need to be protected by a security infrastructure and individual knowledge and responsibility.
- The heads of this university and all members have to participate in the overall security to protect university assets – within an acceptable level of residual risk.

Signed: The boss

Such a policy is the legal base for all company internal security plans, budgets, processes and installations. How could a security policy for your home infrastructure look like? What can you derive from this example about network organization?

SANS has policy templates available: http://www.sans.org/resources/policies/

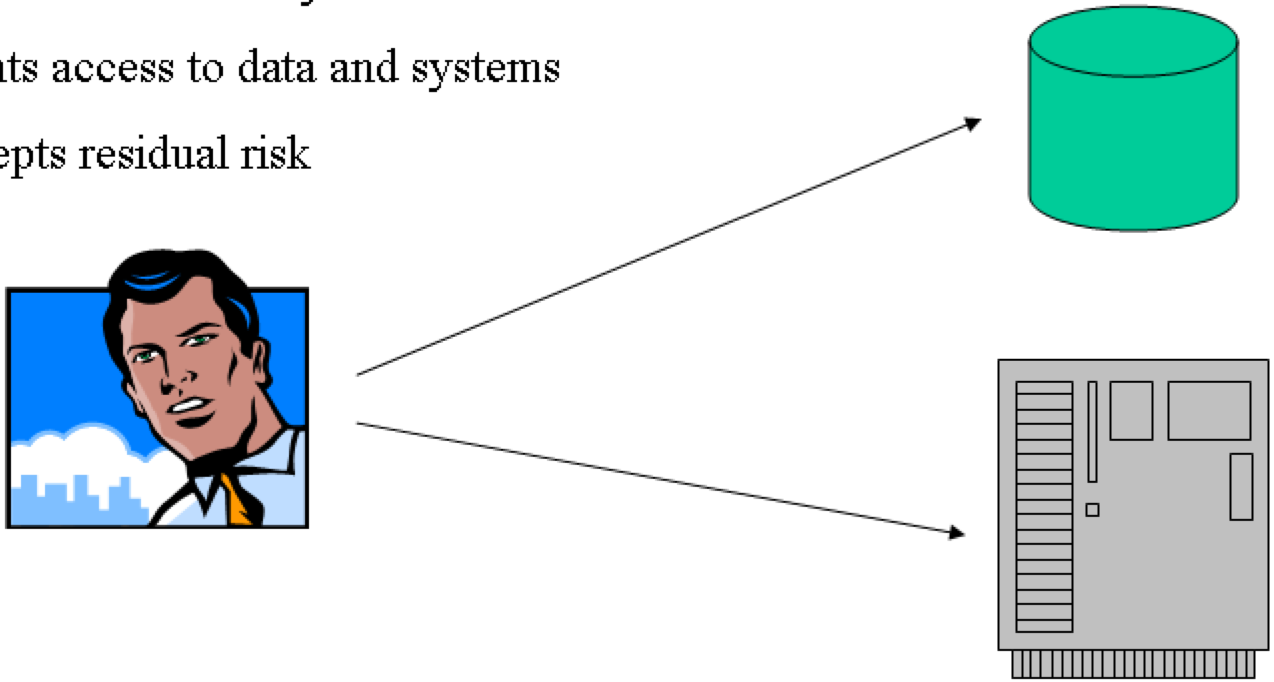
1st. Level Fundamental Policies

- Mandatory asset ownership
- Mandatory data classification
- Confidentiality, Integrity, Availability, Non-Repudiation
- Separation of power/duties
- „Need-to-know“ and „Need-to-do“:
- Risk Management
- Monitoring
- Incident handling

On top of those fundamental rules, the policy defines responsibilites, e.g. that line mangement is also responsible for their employees. Those Rules are MUCH more concrete than you can probably imagine right now!

Mandatory Asset Ownership

- Classifies data and systems
- Grants access to data and systems
- Accepts residual risk



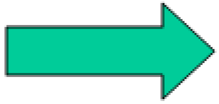
e.g. level one
(internal use)

e.g. trusted vs.
not-trusted

Every asset (data, system, software) has an owner who is responsible for its security. ONLY the owner is allowed to delegate rights to others. This delegation needs to be monitored and archived through a controlled authorization process.

Mandatory Data Classification

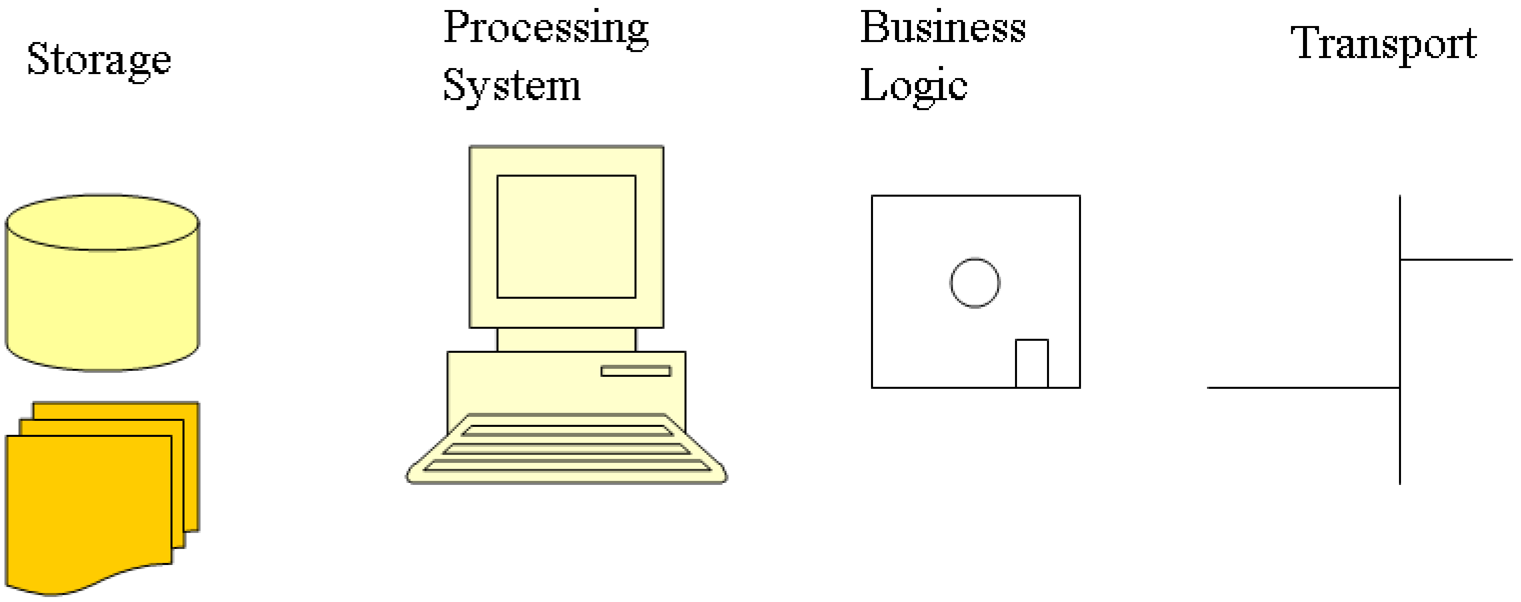
- public data
- internal use only data
- confidential data
- strictly confidential data
- secret data
- top-secret data



- transmission rules (internal/external), e.g. encrypted
- data storage rules (e.g. on systems without networks)
- data handling rules: e.g. never put on computing equipment, store deep inside mountains etc.

Every data asset is subject to classification. Usually 4 or 5 levels of protection are defined. From this classification all security handling rules are derived. The first question at software or computing systems is always: what data classification level are they supposed to handle. BTW: „public“ data does NOT mean unprotected. In most cases at least change control needs to be applied! (e.g. „defacing“ protection)

Confidentiality, Integrity, Availability, Non-Repudiation



Storage

Processing System

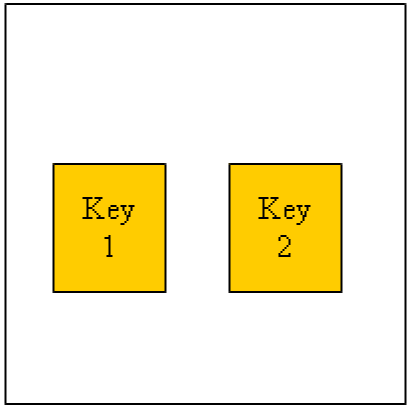
Business Logic

Transport

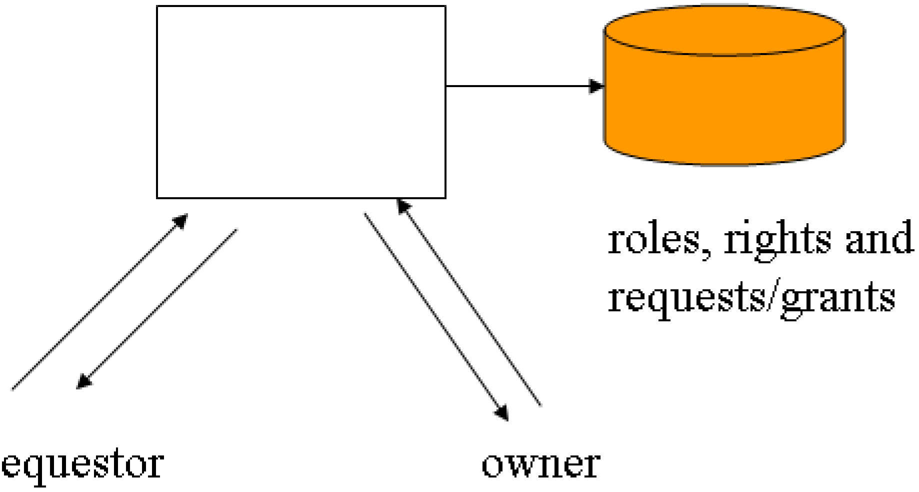
No matter how data are stored, handled or transported: Confidentiality, Integrity, Availability, Non-Repudiation must be guaranteed in relation to the classification of an asset. The first steps in a risk analysis deal e.g. with how a piece of software handles these issues and what risks are involved. Questions to ask are: if data X of level Y is transported across public networks: do they need to be encrypted or is it enough to assure integrity? BTW: can you come up with a classification of your home data (including mails) and how you would like to see them handled?

Separation of Power

Safe/money tresor



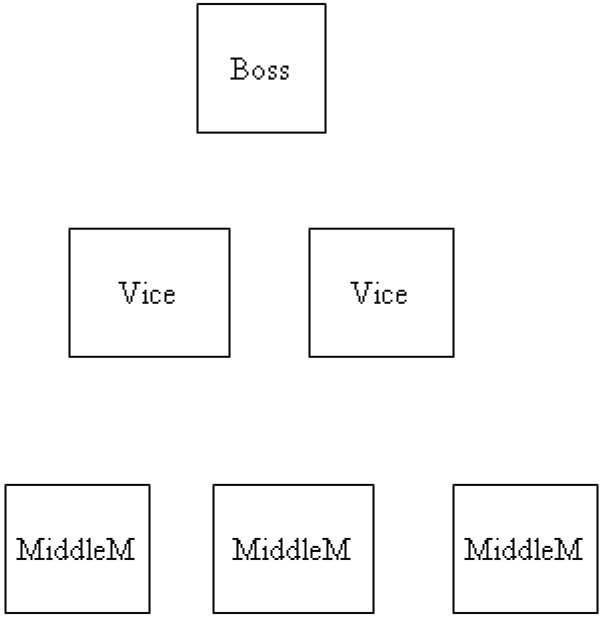
central authorization



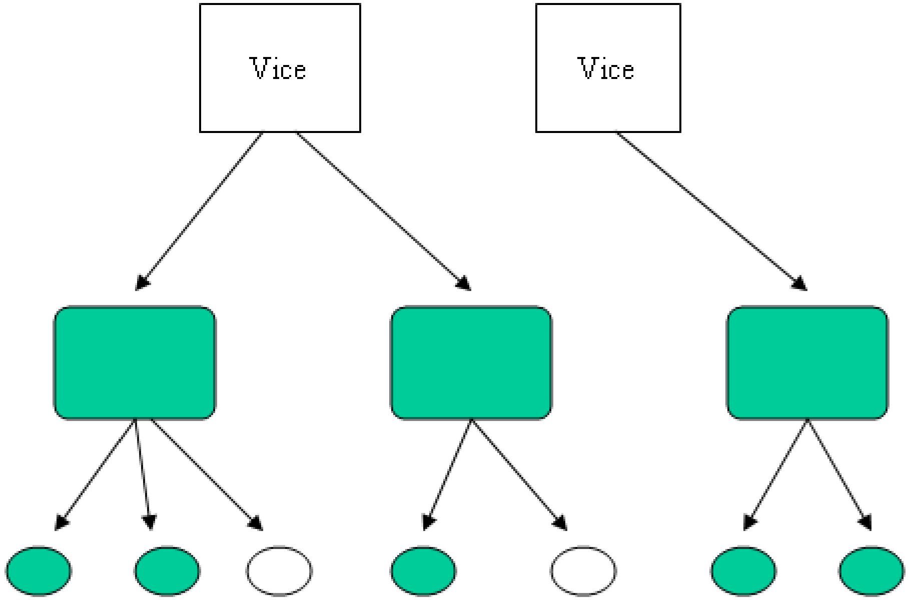
Separation of power/duties: Beyond a certain classification level no single person is allowed to control an asset exclusively. (data or software: This means e.g. that the person that granted a right is not allowed to use it or that a developer cannot acces productive systems). The famous „4-eyes-principle. This has major effects on application design! Think about exceptions in case of emergencies!

Access Control: „Need to Know/Do“

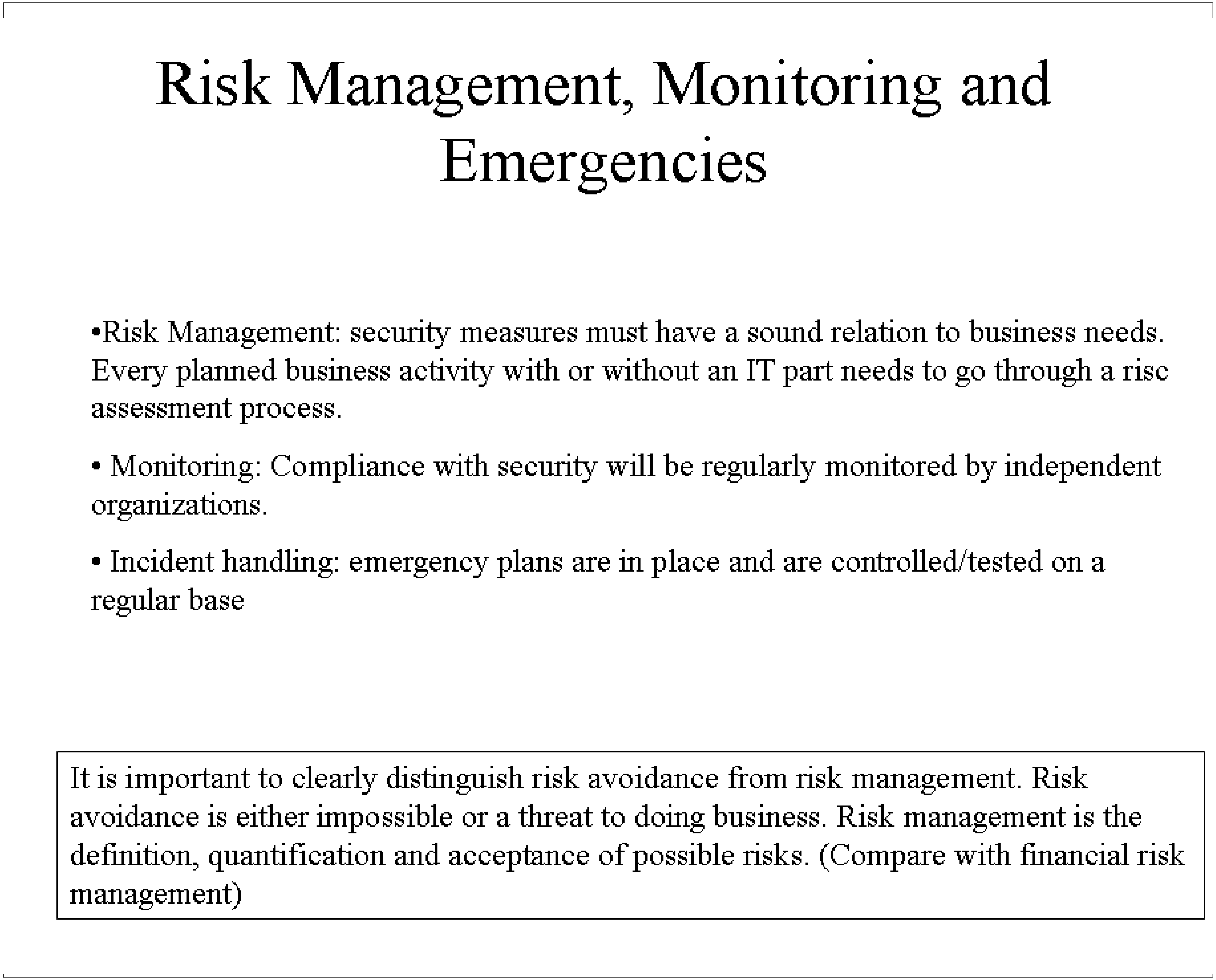
Hierarchical Access Control
(inclusive)



Role Based Access Control
(function based)



„Need-to-know“ and „Need-to-do“: a person should only receive rights necessary for her work – no global or hierarchical authorization. RBAC allows fine grained association of resources, rights and users. At the price of higher complexity. Why should a RBAC system be implemented as a centralized service? How do applications fit into this scheme?



Risk Management, Monitoring and Emergencies

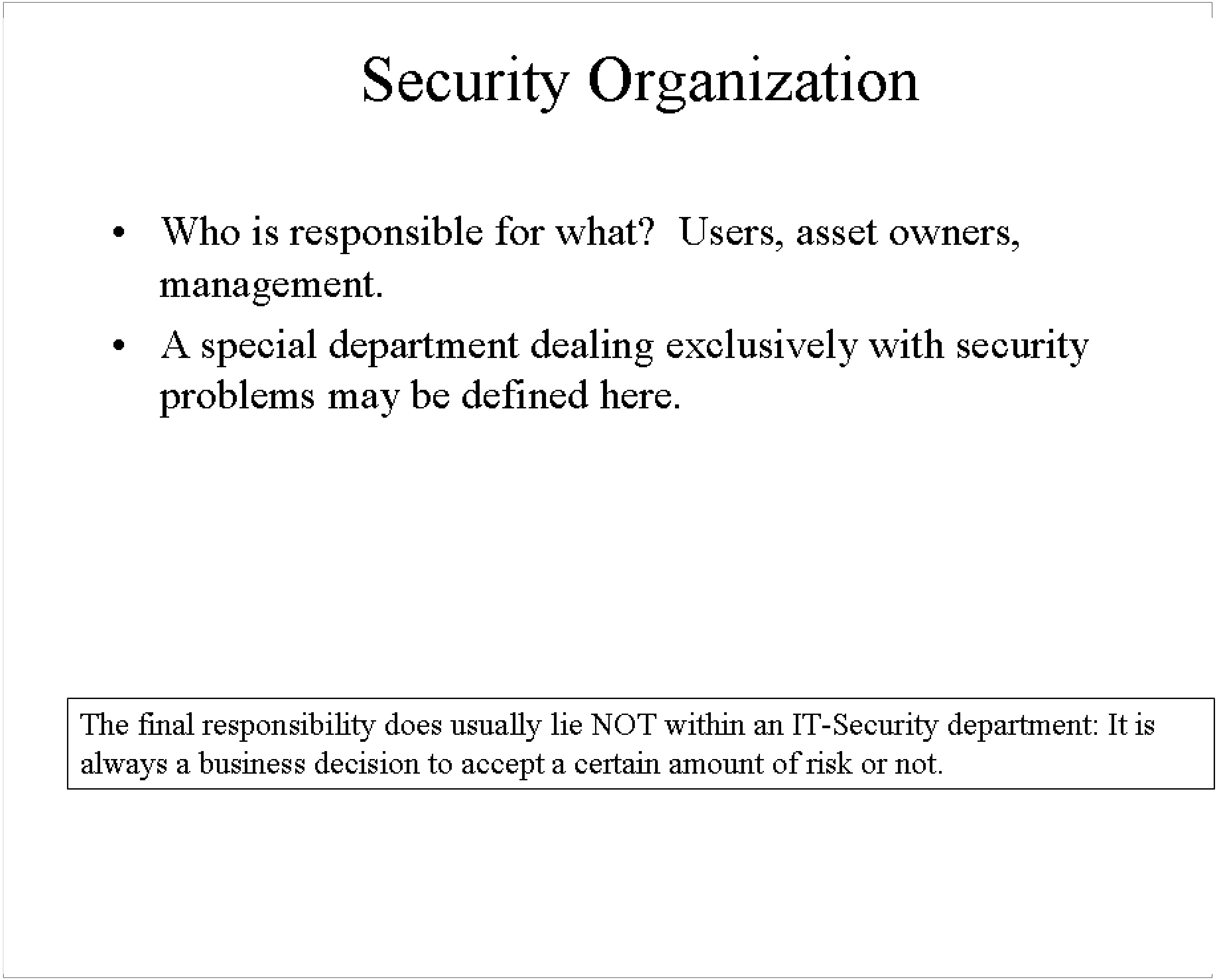
- Risk Management: security measures must have a sound relation to business needs. Every planned business activity with or without an IT part needs to go through a risc assessment process.
- Monitoring: Compliance with security will be regularly monitored by independent organizations.
- Incident handling: emergency plans are in place and are controlled/tested on a regular base

It is important to clearly distinguish risk avoidance from risk management. Risk avoidance is either impossible or a threat to doing business. Risk management is the definition, quantification and acceptance of possible risks. (Compare with financial risk management)

2nd level functional policies

- Security Organization
- Risk Analysis
- Data and Risk
- Hardware and Software Security
- Network Security/Internet Services Security
- Physical Security
- Education
- Disaster Handling

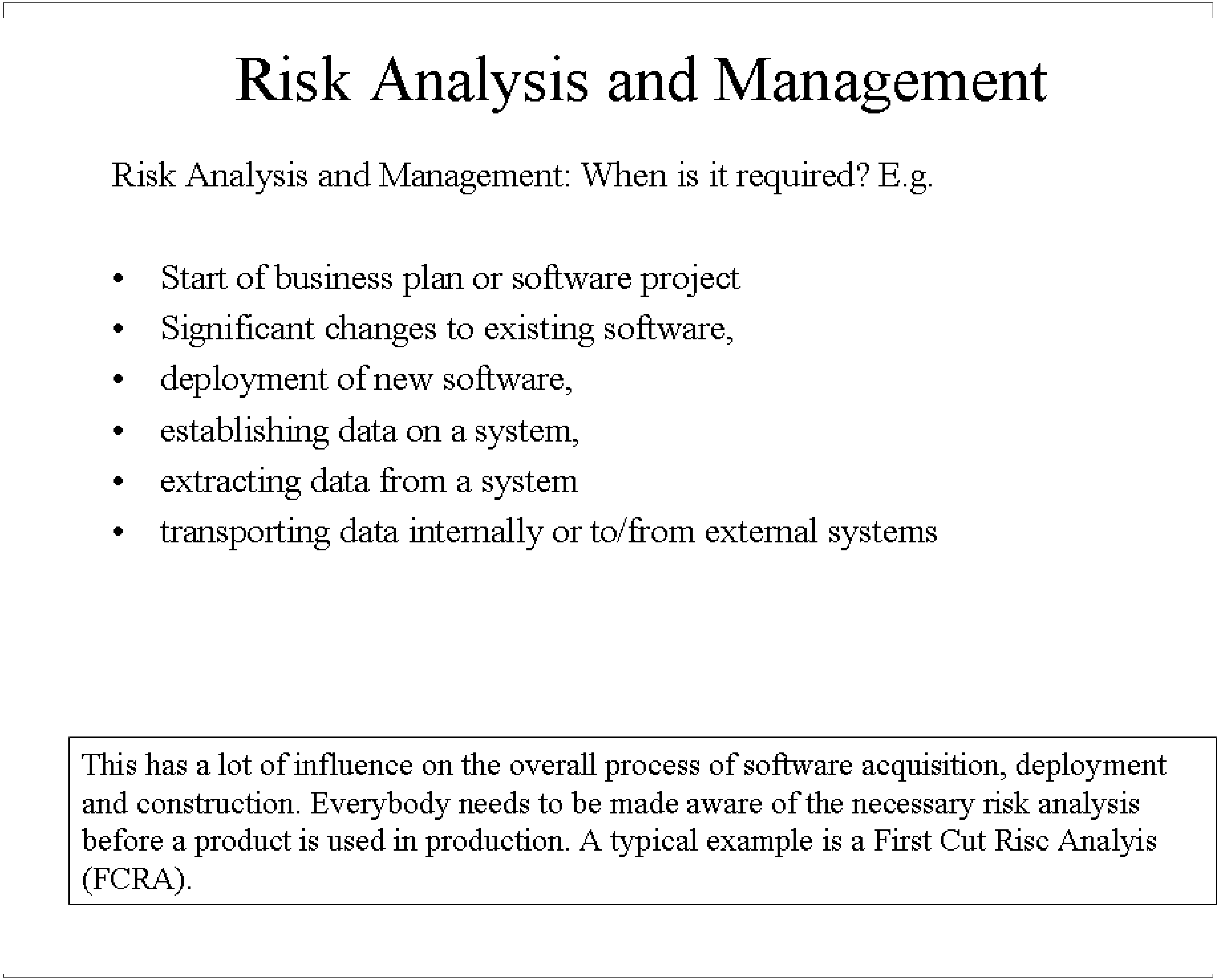
Functional policies are a further drill-down of fundamental policies and principles. Basic processes are defined as well, e.g. in case of software changes.



Security Organization

- Who is responsible for what? Users, asset owners, management.
- A special department dealing exclusively with security problems may be defined here.

The final responsibility does usually lie NOT within an IT-Security department: It is always a business decision to accept a certain amount of risk or not.



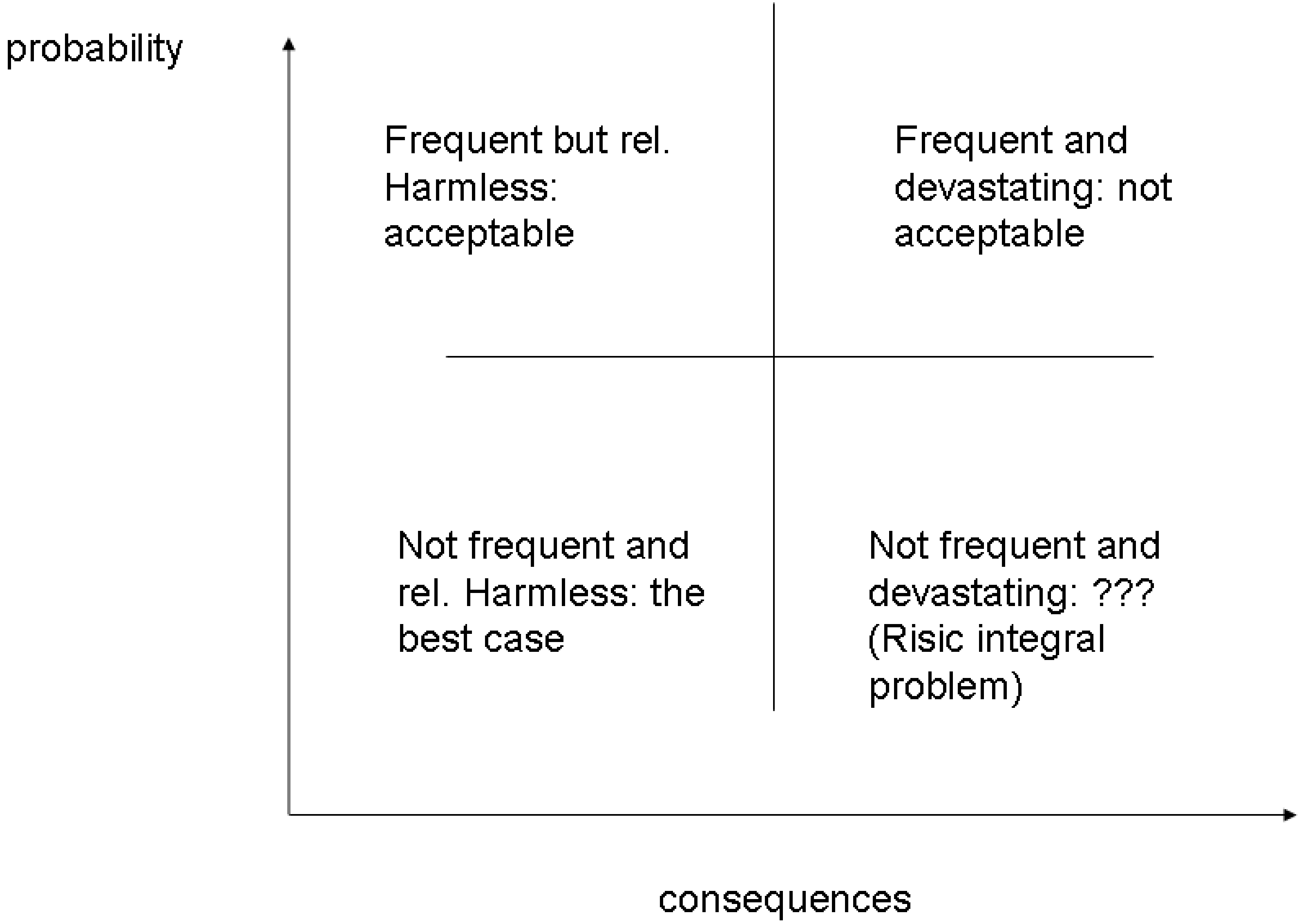
Risk Analysis and Management

Risk Analysis and Management: When is it required? E.g.

- Start of business plan or software project
- Significant changes to existing software,
- deployment of new software,
- establishing data on a system,
- extracting data from a system
- transporting data internally or to/from external systems

This has a lot of influence on the overall process of software acquisition, deployment and construction. Everybody needs to be made aware of the necessary risk analysis before a product is used in production. A typical example is a First Cut Risc Analyis (FCRA).

Damage vs. Likelihood



probability

Frequent but rel. Harmless: acceptable

Frequent and devastating: not acceptable

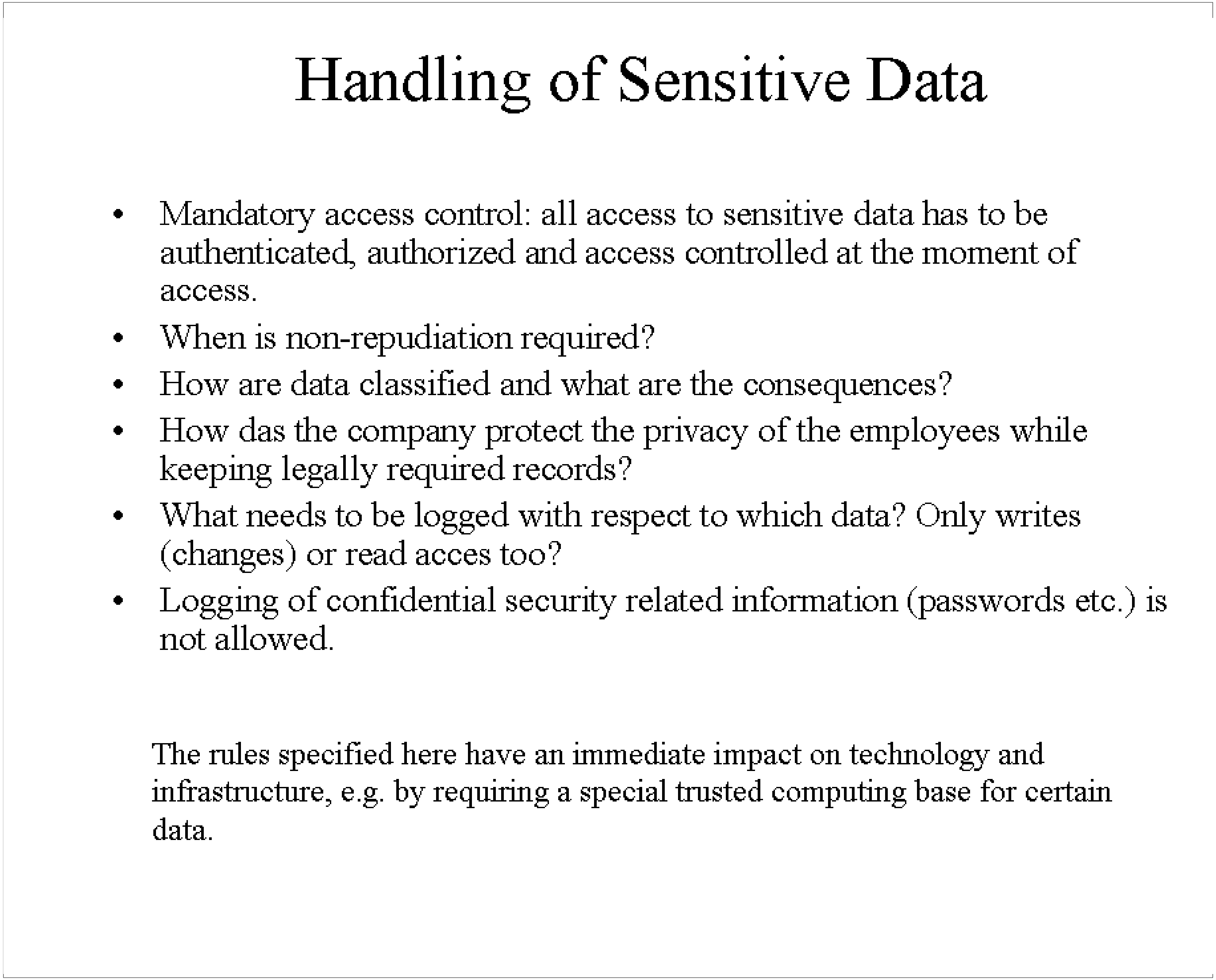
Not frequent and rel. Harmless: the best case

Not frequent and devastating: ??? (Risic integral problem)

consequences

First Cut Risc Analysis (FCRA)

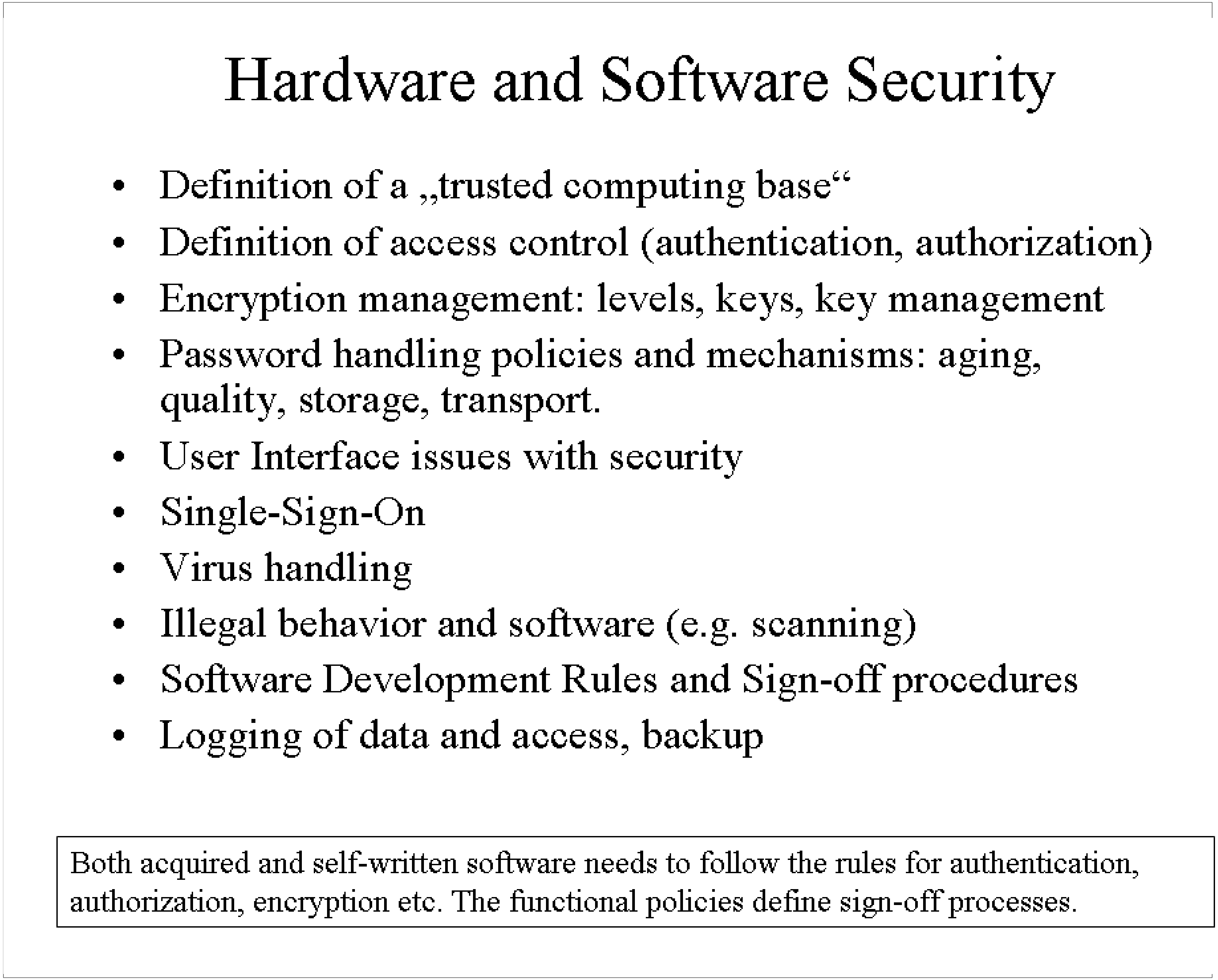
Threat	Frequence	Damage	Result
Forged tickets	Rare	small	Accept risc
Stolen Cards	More often	Small	Accept risc
DOS Attack on Service	Frequent	Small	Accept risc



Handling of Sensitive Data

- Mandatory access control: all access to sensitive data has to be authenticated, authorized and access controlled at the moment of access.
- When is non-repudiation required?
- How are data classified and what are the consequences?
- How das the company protect the privacy of the employees while keeping legally required records?
- What needs to be logged with respect to which data? Only writes (changes) or read acces too?
- Logging of confidential security related information (passwords etc.) is not allowed.

The rules specified here have an immediate impact on technology and infrastructure, e.g. by requiring a special trusted computing base for certain data.



Hardware and Software Security

- Definition of a „trusted computing base“
- Definition of access control (authentication, authorization)
- Encryption management: levels, keys, key management
- Password handling policies and mechanisms: aging, quality, storage, transport.
- User Interface issues with security
- Single-Sign-On
- Virus handling
- Illegal behavior and software (e.g. scanning)
- Software Development Rules and Sign-off procedures
- Logging of data and access, backup

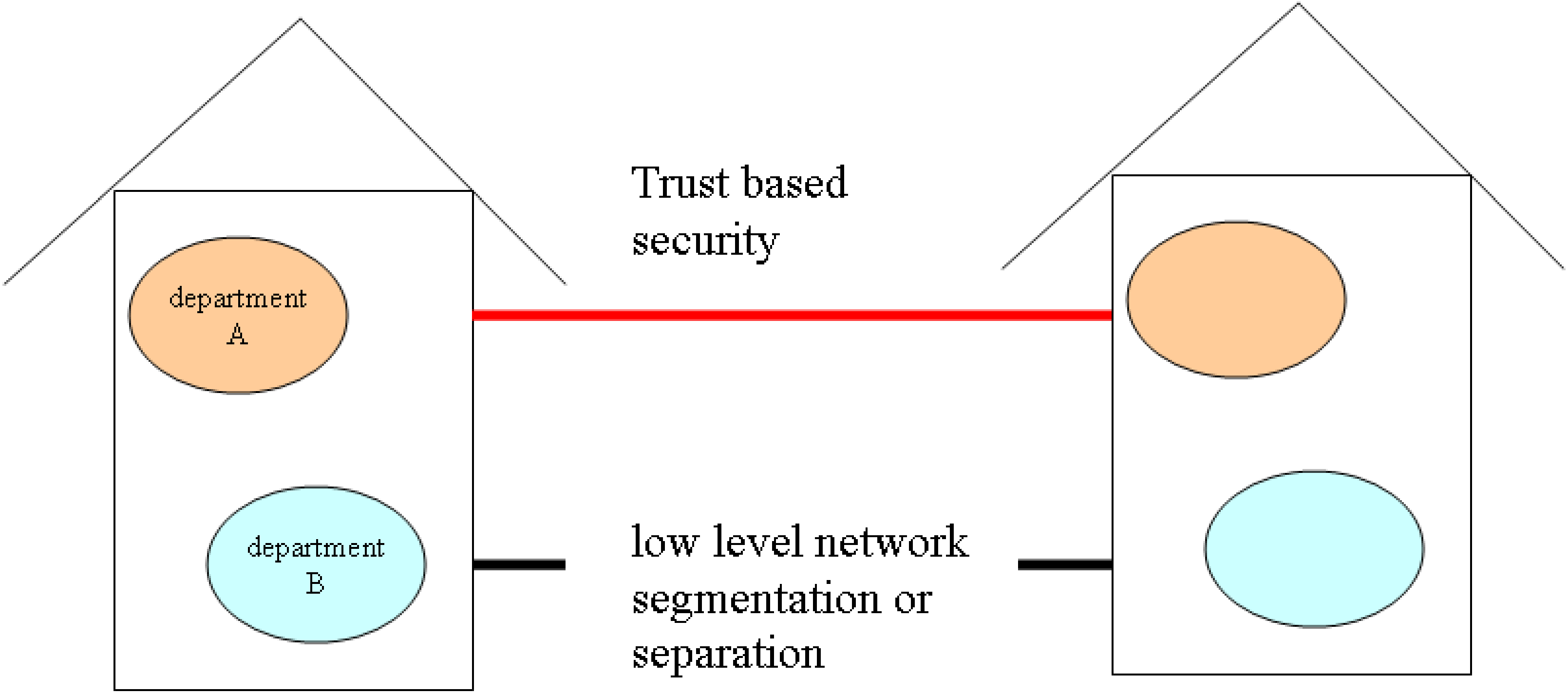
Both acquired and self-written software needs to follow the rules for authentication, authorization, encryption etc. The functional policies define sign-off processes.

Network Security

- Who can connect machines to the company network?
- Definition and border of the company intranet/extranet/internet connections
- Dial-up security
- End-to-end security (application level over session level over link-level encryption)
- Mandatory firewalls between private and public networks
- Mandatory firewalls between divisions for legal and other reasons
- E-mail regulations (no confidential data, encryption, mandatory virus checks)
- Download rules and procedures

The trend is here from perimeter based security (like a fence in old times) to security zones of different quality (like in airports) to ever more fine-grained forms of security be certificates, VPNs and so on. Finally this raises the question: what is the border of a company in digital times?

Network security which no longer works



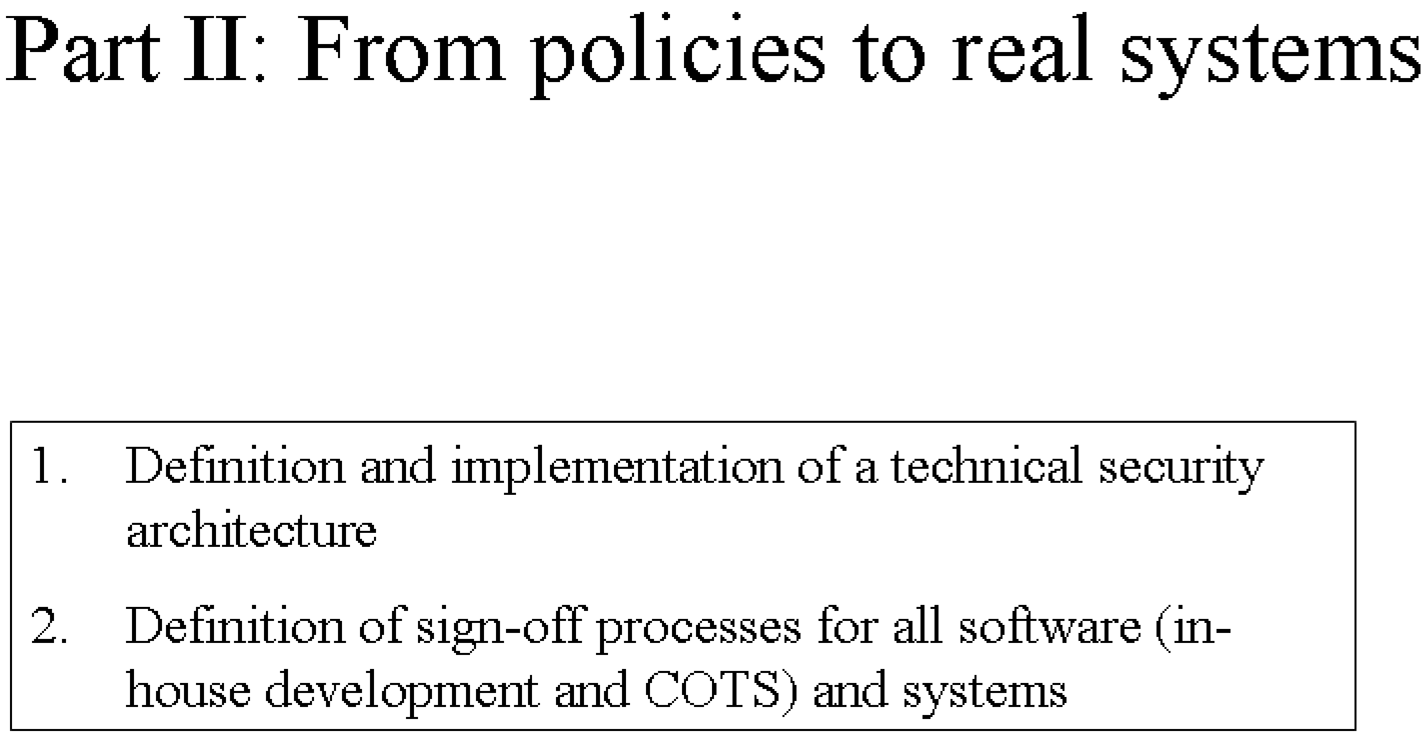
Trust based security in networks breaks down as soon as somebody not-to-be-trusted enters the environment. Low level segmentation requires clear borders. Modern business changes too fast for those techniques to survive: A department is split in two halves residing in different locations: formerly separated networks now need to be connected. Trust based security cannot deal with the newcomers.

This means that the required flexibility needs to be achieved differently: Virtual Private Networks, private VLANs based on programmable switches etc. Business change put a lot of pressure on network security – but not only on those as we will see with access control systems.

Last but not least:

- Physical Security: establish physically secured environments for systems in the trusted computing base
- Education: make classes on IT-security mandatory. Use Intranet to warn and educate users (e.g. virus threats)
- Disaster Handling: Have detailed plans for break-ins and attacks.

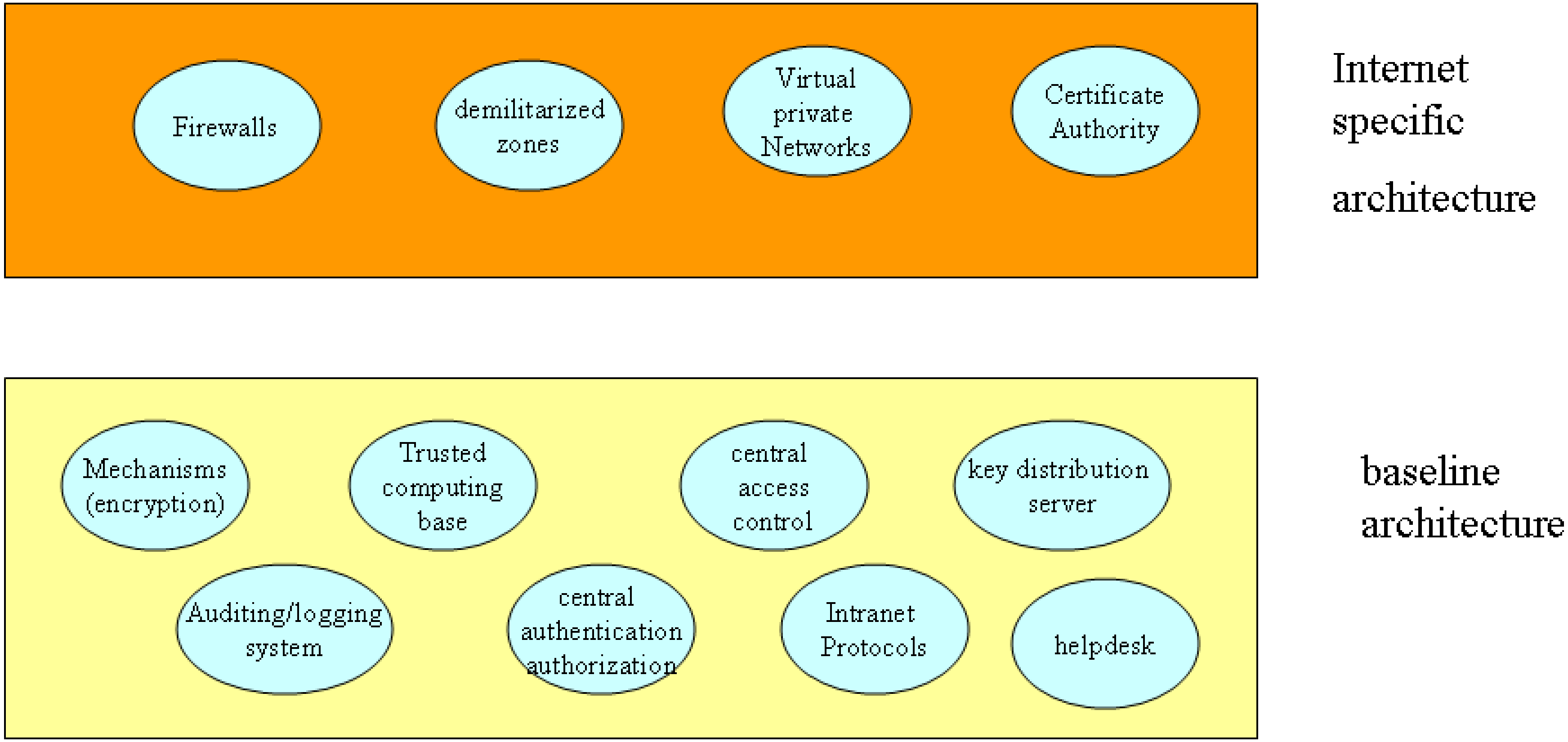
„soft“ security like education and legal warnings or requests for compliance are still necessary as not all aspects of security can be covered by technology. It is very important to understand the limitations of technology. For every business application in production there needs to be a document describing the business organization or the special tasks necessary to preserve the security of the solution.



Part II: From policies to real systems

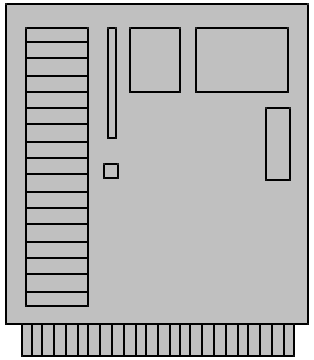
1. Definition and implementation of a technical security architecture
2. Definition of sign-off processes for all software (in-house development and COTS) and systems

Technical Architecture



Before using the internet, every company needs to establish a baseline security architecture. Otherwise every new PC/workstation would have to go through a separate security analysis. By defining standards and providing central services a company can save on infrastructure costs while still maintaining security.

Trusted Computing Base



full access control management (e.g. administration under real user id)

special middleware (if at all)

special operating system

logging and auditing of all actions

full system management control

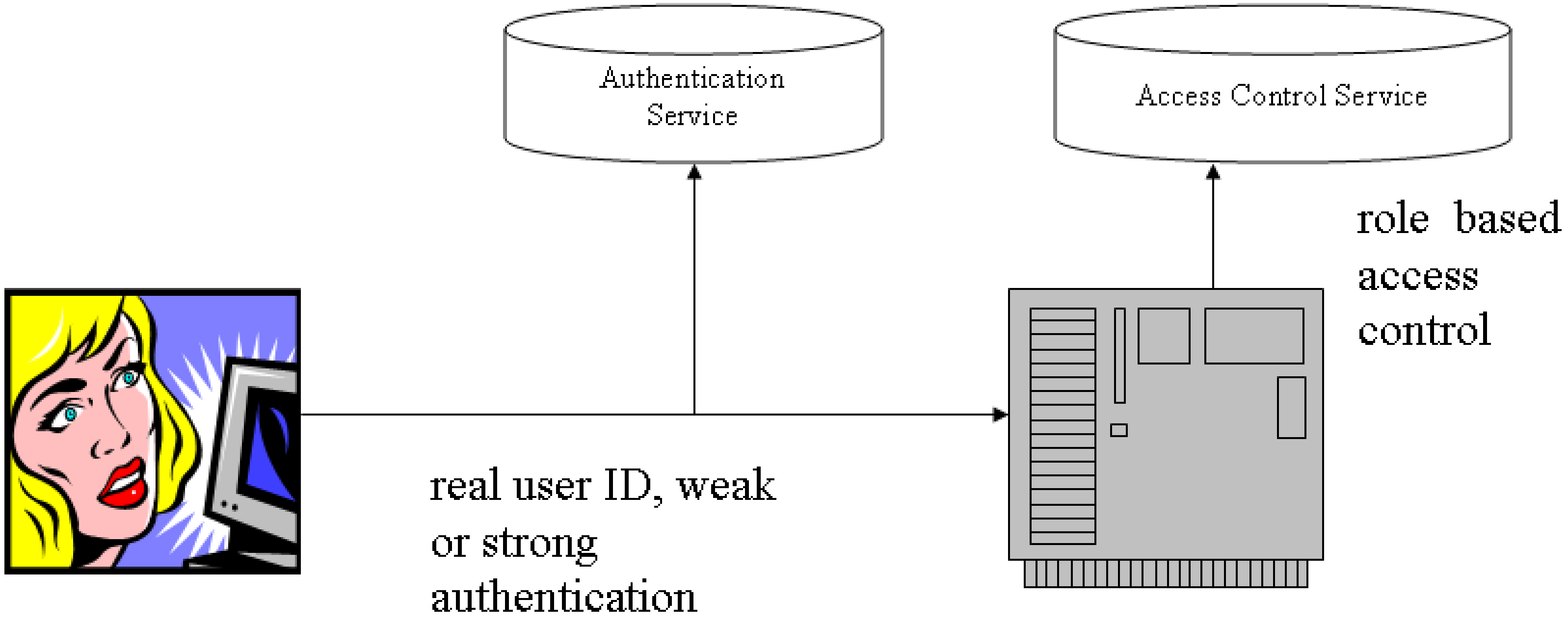
hardware based authentication

link level encryption

all software under change management and monitoring

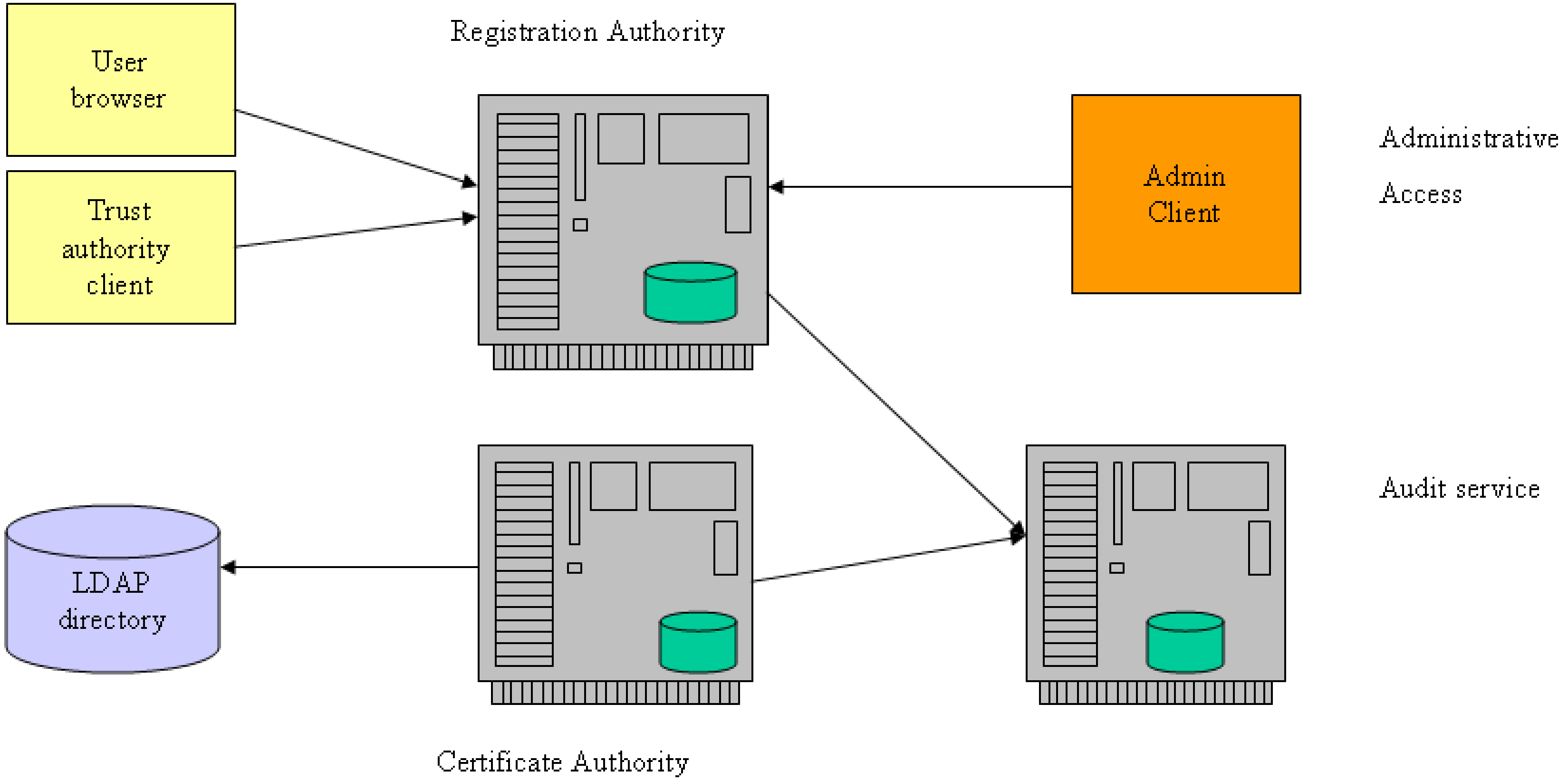
Characteristics of a trusted computing base are that classified data can be stored or processed on these systems. An authentication acquired on such a system „counts“ as a real one and can be delegated – something that is not allowed on PC-front ends. Don‘t confuse a trusted base with a trust-based relation: Systems in the trusted base DO AUTHENTICATE themselves if they use remote functions. Logging and auditing needs to happen on trusted systems.

Authentication and Access Control


Authentication Service
Access Control Service
role based access control
real user ID, weak or strong authentication

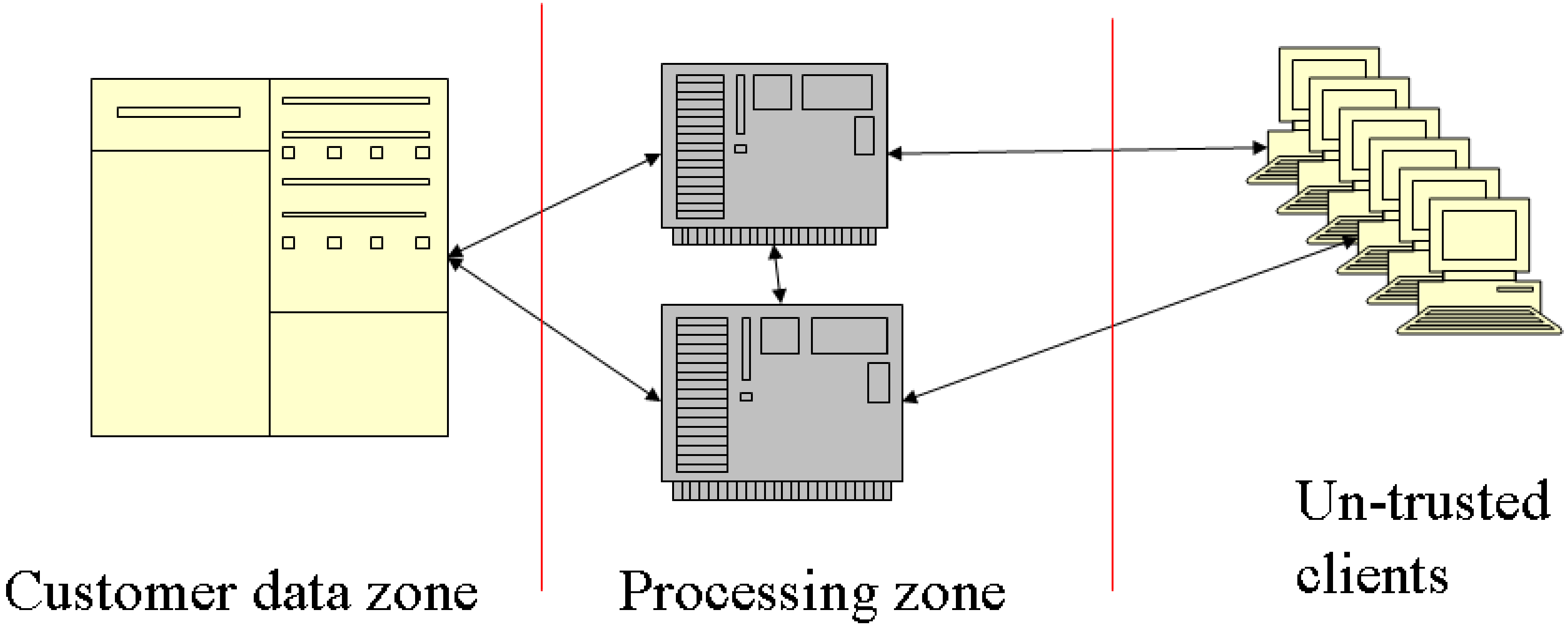
The functional policies for access control define central services which have to be used. The use of functional user IDs may be explicitly forbidden. (What is the higher principle behind this request?)

Certificate Authority



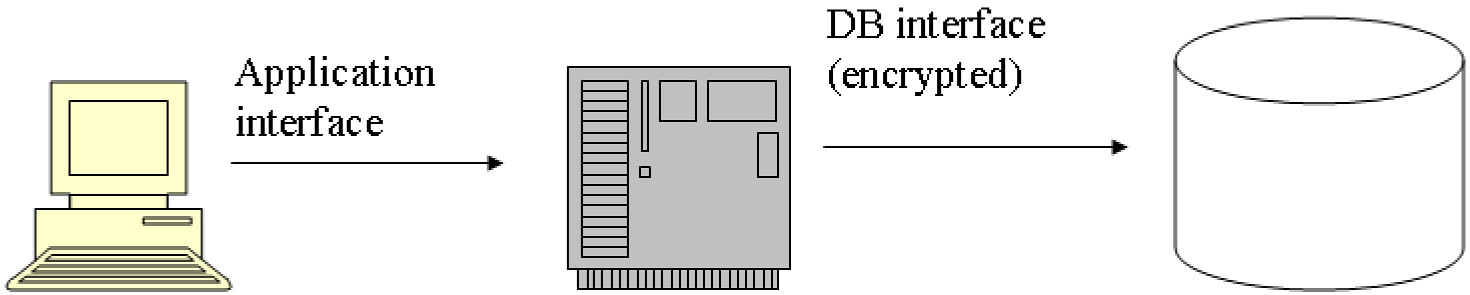
One example for a certificate authority. See Websphere Security Redbook for more details. Distributing certificates is one way to achieve strong authentication. A userid/password/Transaction-Number (scratch-number) system provides good external security as well. Systems handling keys, scratch lists etc. are extremely sensitive and need to run on specially trusted systems in special physical environments. (Where do you place the master key?) What if somebody loses a key? How many keys do you need?

Data vs. Processing locations



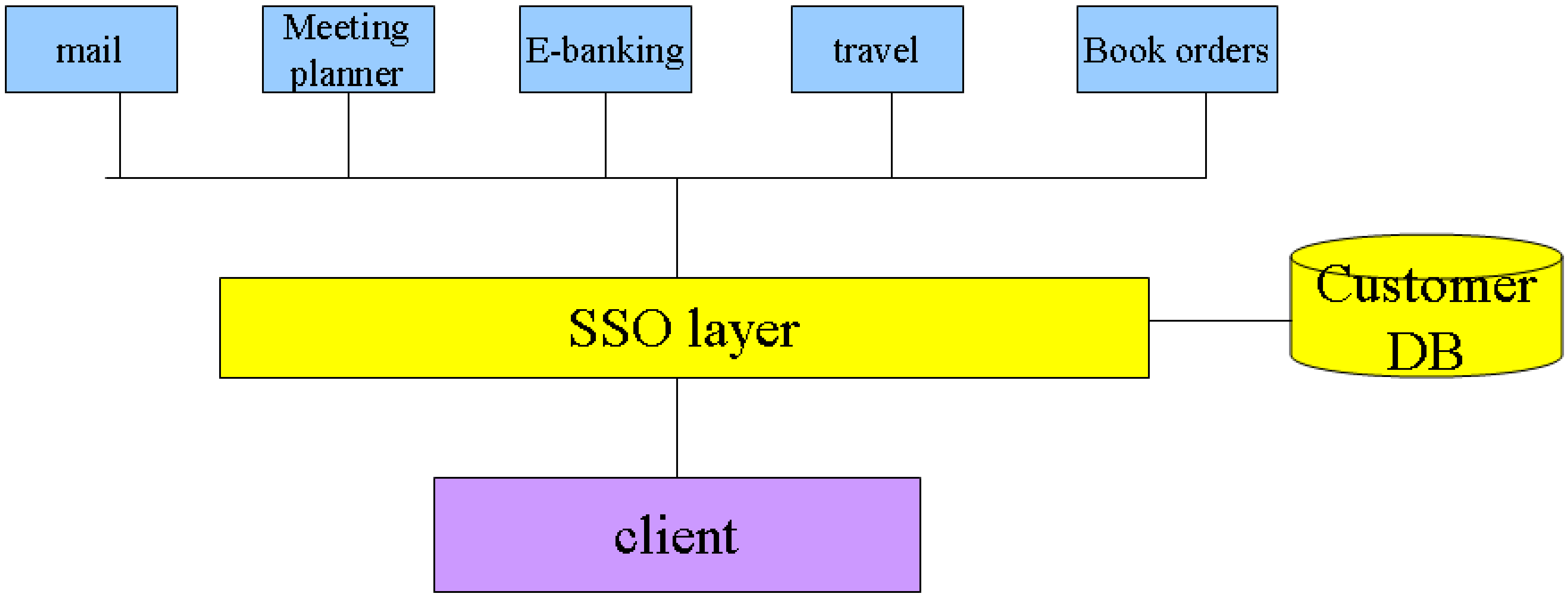
Many companies use a distributed system to distribute data and processing. All sensitive data are stored on the backend systems and will be only exported for processing if authentication/authorization and encryption levels are apropriate. In many large companies this is the initial structure when business wants to put services and data „on the web“. A web infrastructure needs to somehow fit into the whole picture.

No direct DB access



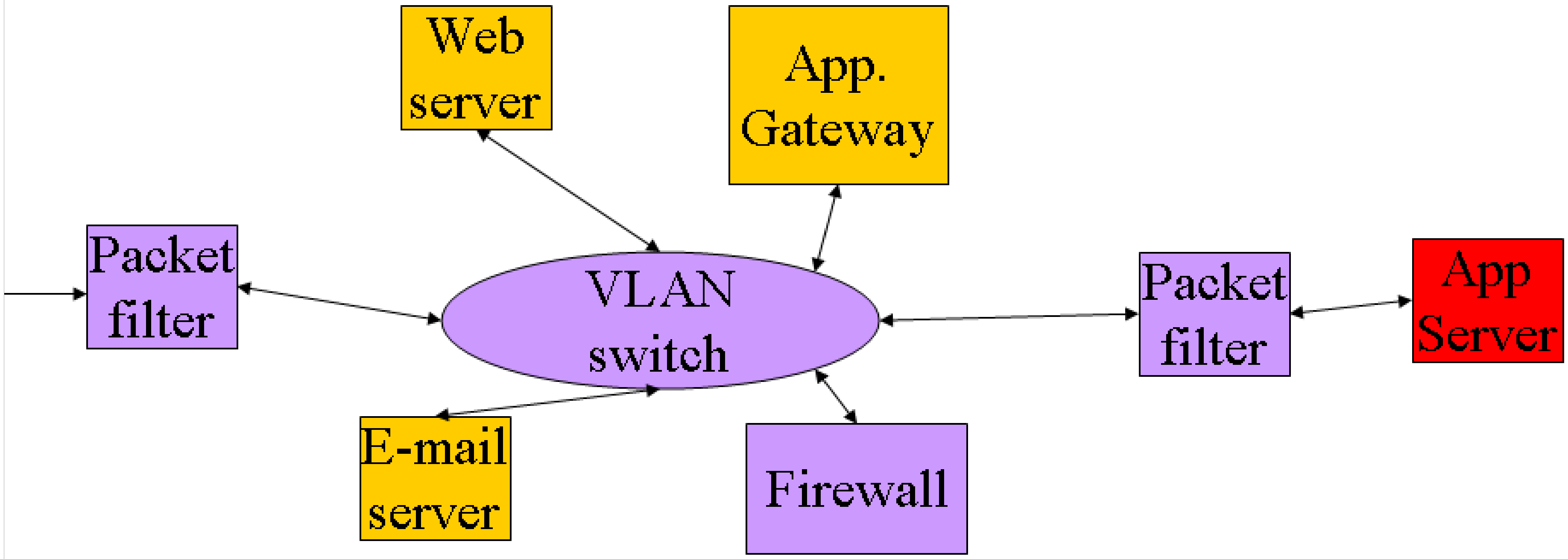
Two tier applications or monolithic applications are not allowed to access databases directly. All access has to go through application interface basically restrict access to known functions. No free SQL statements against DBs are allowed. There are both performance and security reasons behind this type of implementation. You can create a form that asks for specific types of architectures and makes it clear which ones are not to be used (homologation form).

Single Sign-On (SSO)



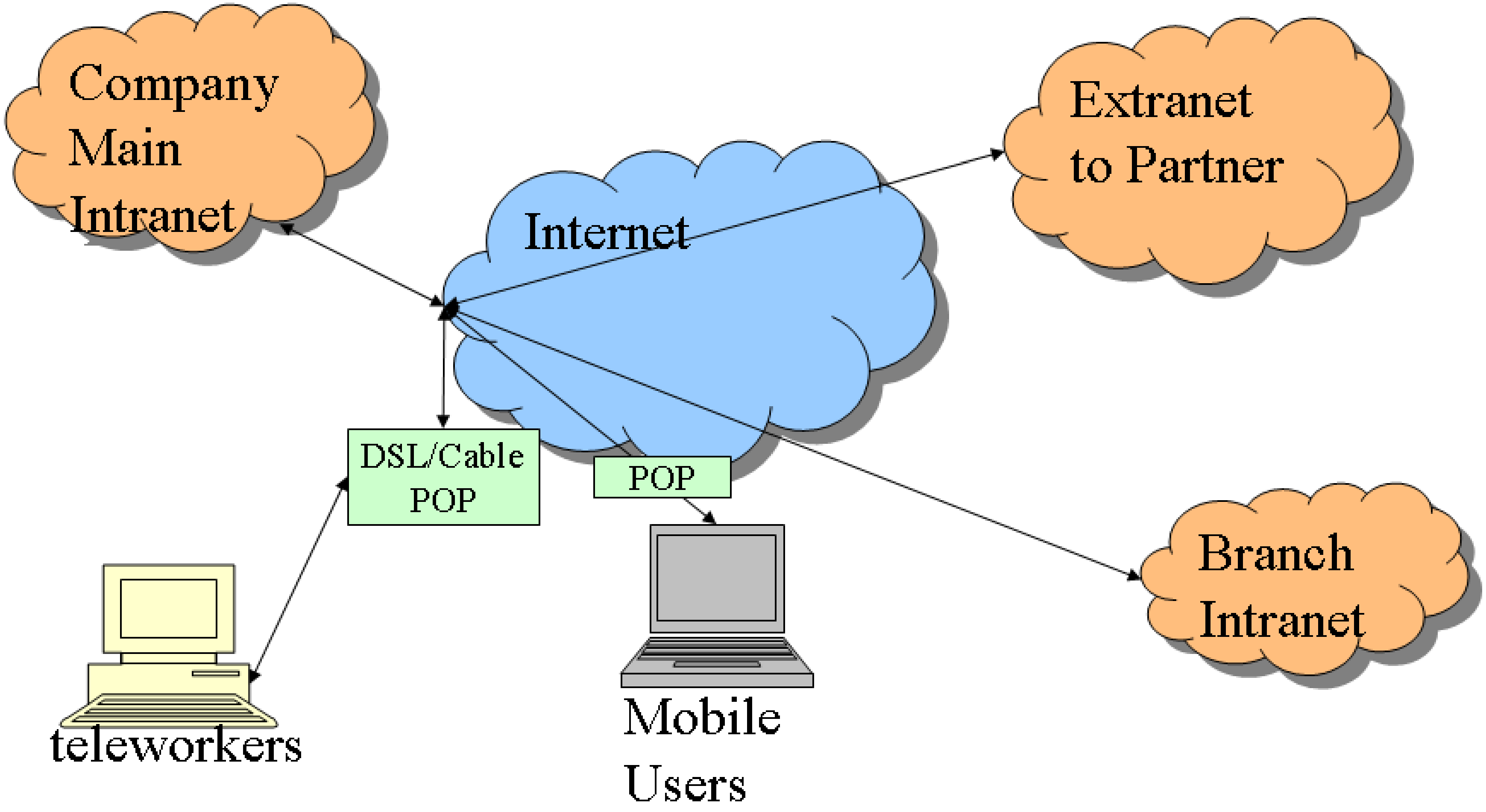
Instead of authenticating with every application the client only authenticates once with the SSO layer. The applications receive the client credentials from the authentication layer. For an example of a SSO product see www.netegrity.com (siteminder). Does SSO have only positive aspects? What about applications? Users?

Demilitarized Zone(s) Architecture



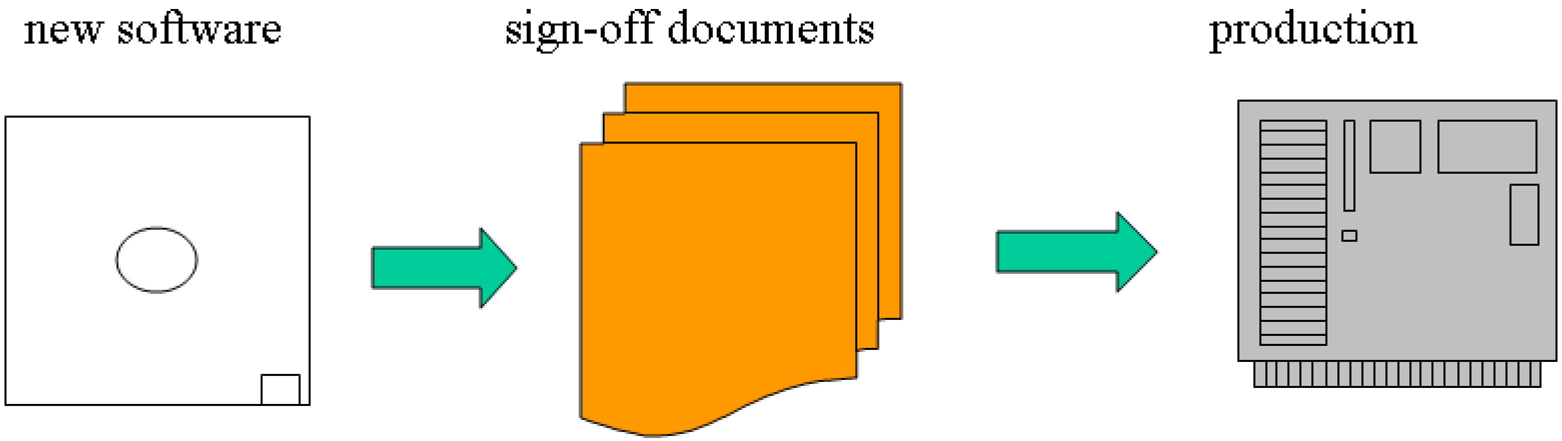
No system is directly connected to the internet. Application traffic needs to pass 2 routers and one application gateway. Configuration is VERY critical. VLAN advantage is the point to point control available. Hardware authentication and hardened systems are paramount in the DMZ. Only a few systems are visible on the Internet. This concept can be extended to several stacked DMZ‘s providing fine grained control.

Virtual Private Network with site-to-site IPsec



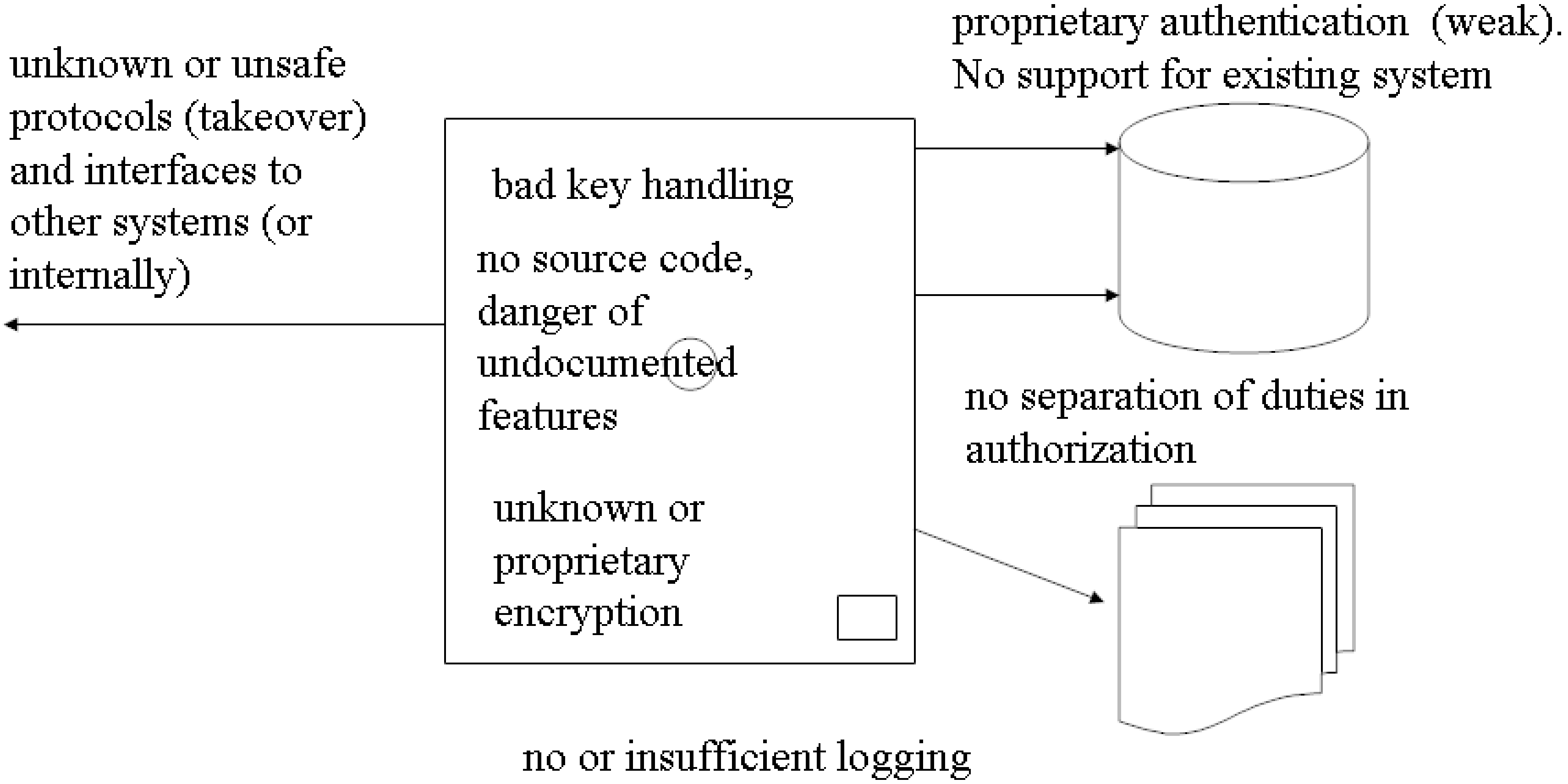
Ipsec allows the creation of a private tunnel across public lines. This includes privacy and protection against traffic analysis. Other options are L2TP, Layer 2 Tunneling Protocol, the followup to MS PPTP. Ipsec includes IKE (Internet Key Exchange) and the concept of secure associations (SA). What about filtering? Auditing? (see SCIP Proxies later)

Ensuring compliance: Sign-Off processes



Nothing goes into production without passing a sign-off process. Sign-off means that all relevant features of an application have been documented and found in compliance with the existing infrastructure and technical security architecture and policies. Actually, the sign-off process starts even BEFORE developments starts: already the software design documents need a sign-off to prevent wrong mechanisms from being implemented. For externally developed software a questionaire checks compliance with company security rules.

Integration Problems with Standard Software



unknown or unsafe protocols (takeover) and interfaces to other systems (or internally)

proprietary authentication (weak). No support for existing system

bad key handling

no source code, danger of undocumented features

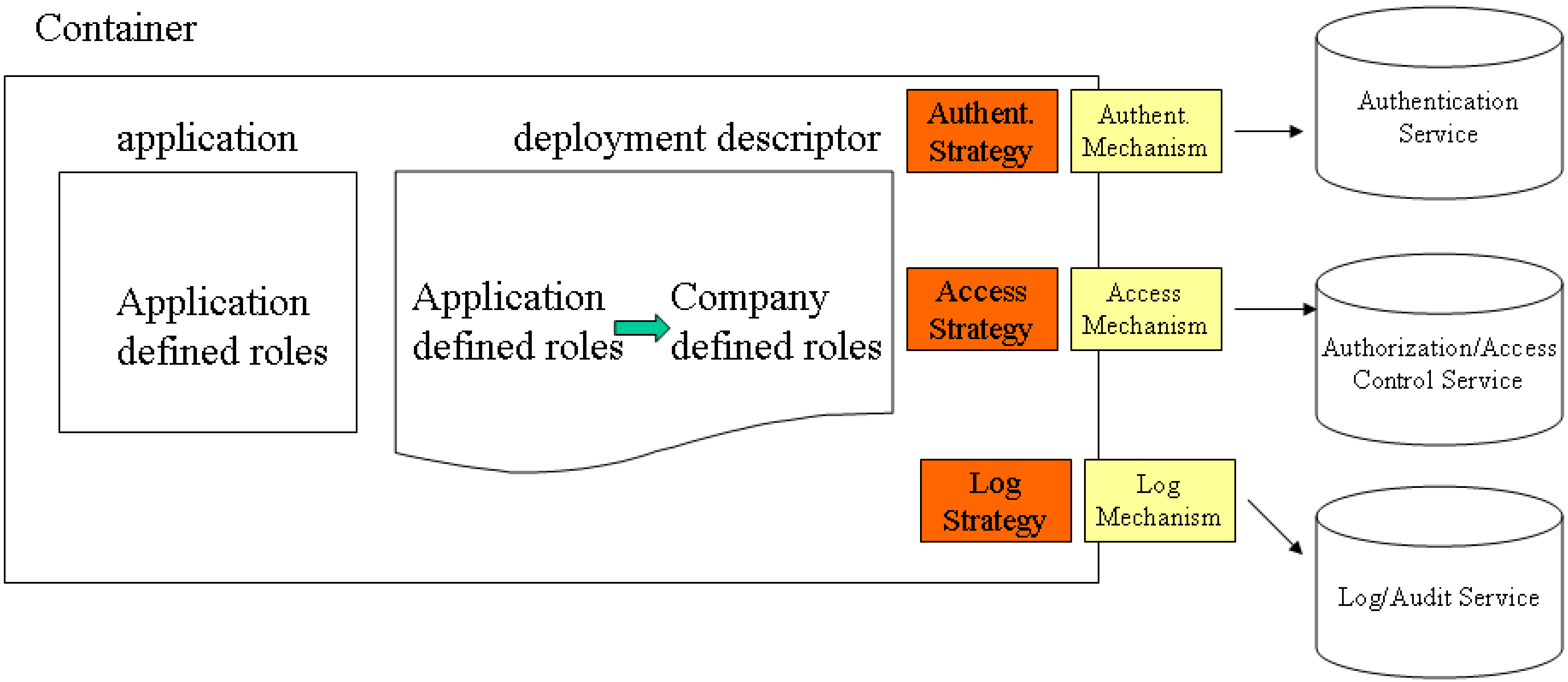
unknown or proprietary encryption

no separation of duties in authorization

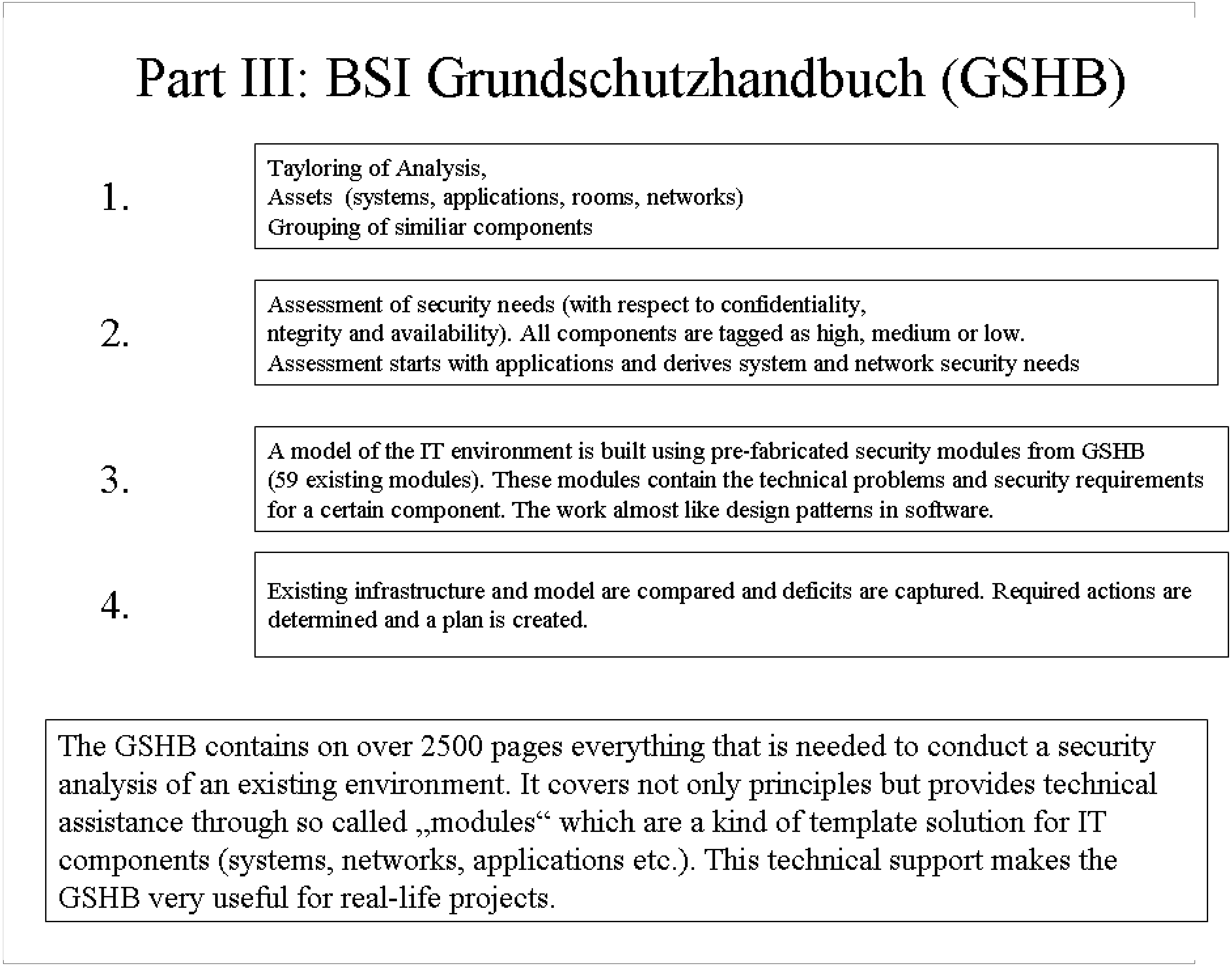
no or insufficient logging

Even security related products have sometimes big security problems. A modern software should have APIs to external interfaces and services for authentication and authorization. It should NOT define its own implementation – or at least no make it mandatory.

Software Design Guidelines for Integration



An application that wants to integrate into existing infrastructure needs a) to externalize user roles so that they can be mapped to existing roles in a specific company. It also needs to factor out WHAT and WHEN security related things happen (using e.g. pluggable strategies) and HOW things have to happen – in other words the mechanisms need to be replaceable as well (bridge pattern). Other rules are: no proprietary encryption algorithms, no backdoors, no super-user etc.



Part III: BSI Grundschutzhandbuch (GSHB)

1. Tayloring of Analysis,
Assets (systems, applications, rooms, networks)
Grouping of similiar components

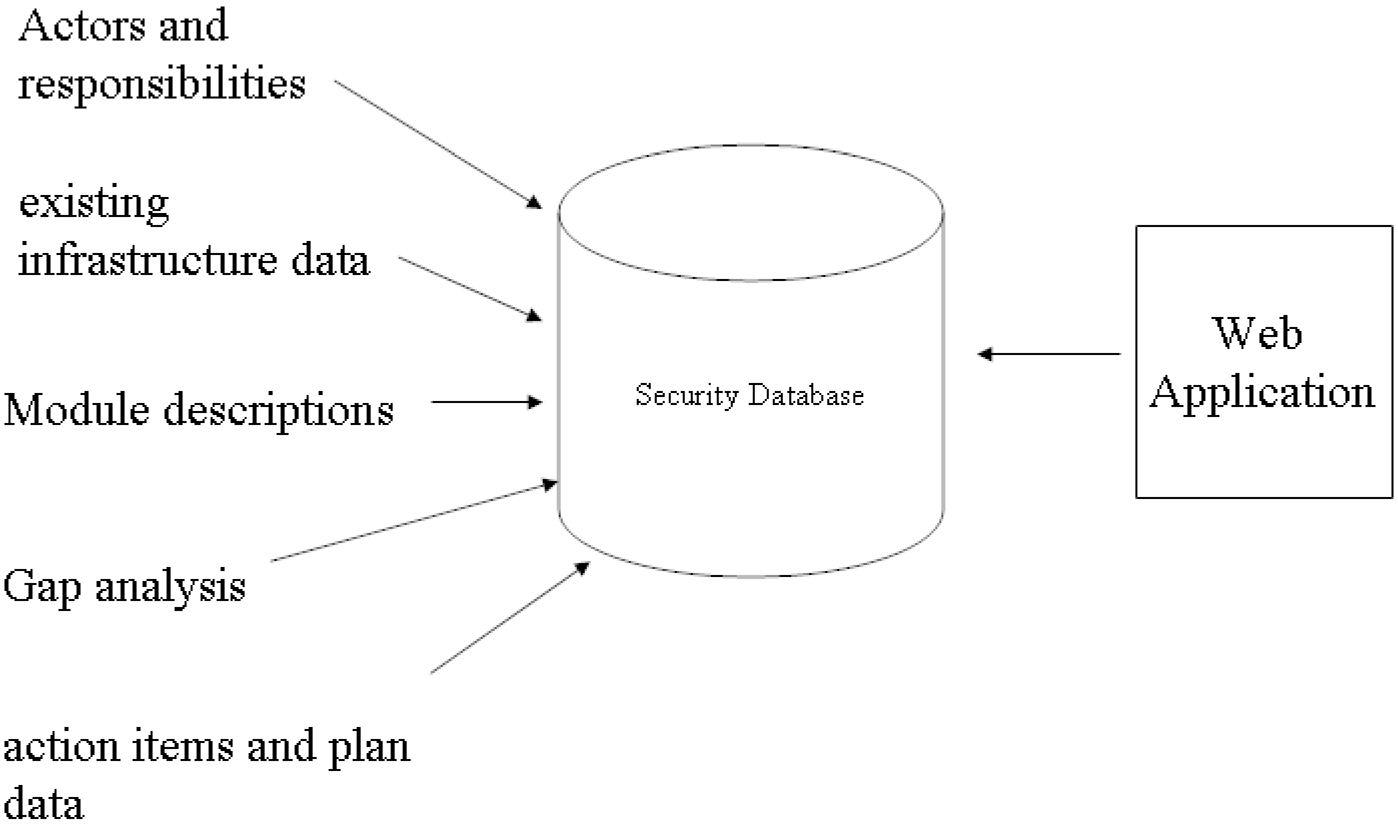
2. Assessment of security needs (with respect to confidentiality,
ntegrity and availability). All components are tagged as high, medium or low.
Assessment starts with applications and derives system and network security needs

3. A model of the IT environment is built using pre-fabricated security modules from GSHB
(59 existing modules). These modules contain the technical problems and security requirements
for a certain component. The work almost like design patterns in software.

4. Existing infrastructure and model are compared and deficits are captured. Required actions are
determined and a plan is created.

The GSHB contains on over 2500 pages everything that is needed to conduct a security analysis of an existing environment. It covers not only principles but provides technical assistance through so called „modules“ which are a kind of template solution for IT components (systems, networks, applications etc.). This technical support makes the GSHB very useful for real-life projects.

Data Handling During Analysis



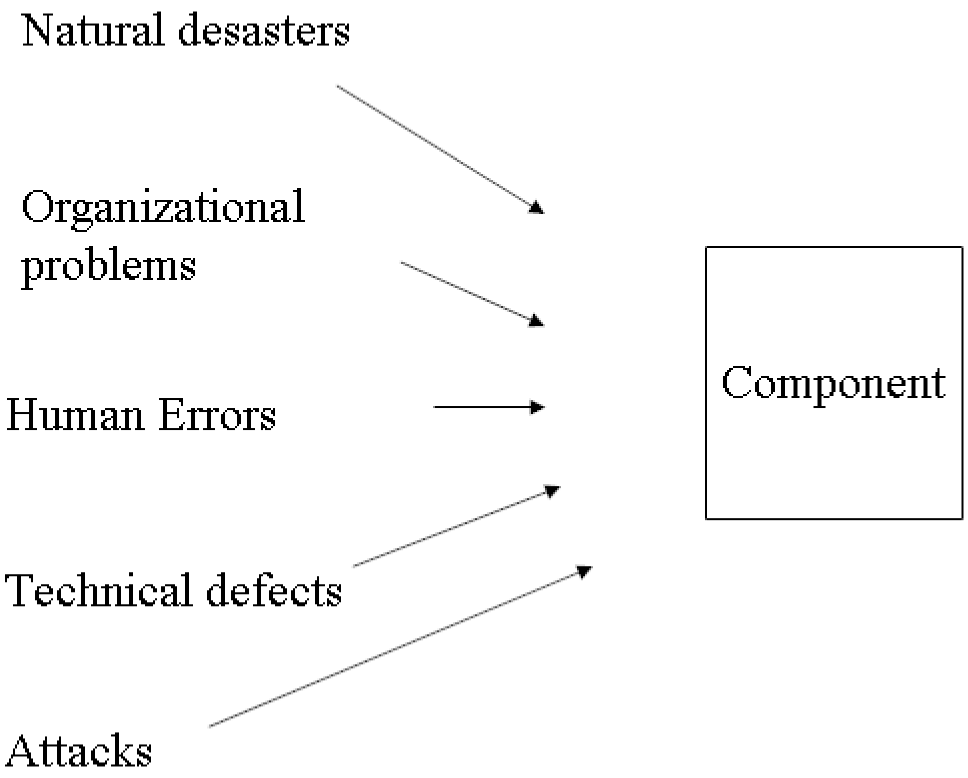
Actors and responsibilities
existing infrastructure data
Module descriptions
Gap analysis
action items and plan data
Security Database
Web Application

To keep data items consistent it is advisable to collect all security related data in a database. To allow the distribution of work every involved employee should be able to work on her assets and store related data in the database. The bsgh module informatinon is available in electronic form and can be used as a skeleton. A small web-application can give lightweight access to the analysis data. A content management system could be used as well.

Experiences from BSGH Usage

- Often availability is the most important security property (typical for collaborative environments)
- The law of maximum security effects leads frequently to many systems/networks being tagged as „critical“. This is a consequence of mixing critical data/transports with non-critical. A segmentation of networks into zones (airport security) is one option here. Or use better end-to-end security (which requires application changes).
- Distribution of services can decrease the security needs of individual servers. Cumulation of uncritical services can increase the security needs of a server.

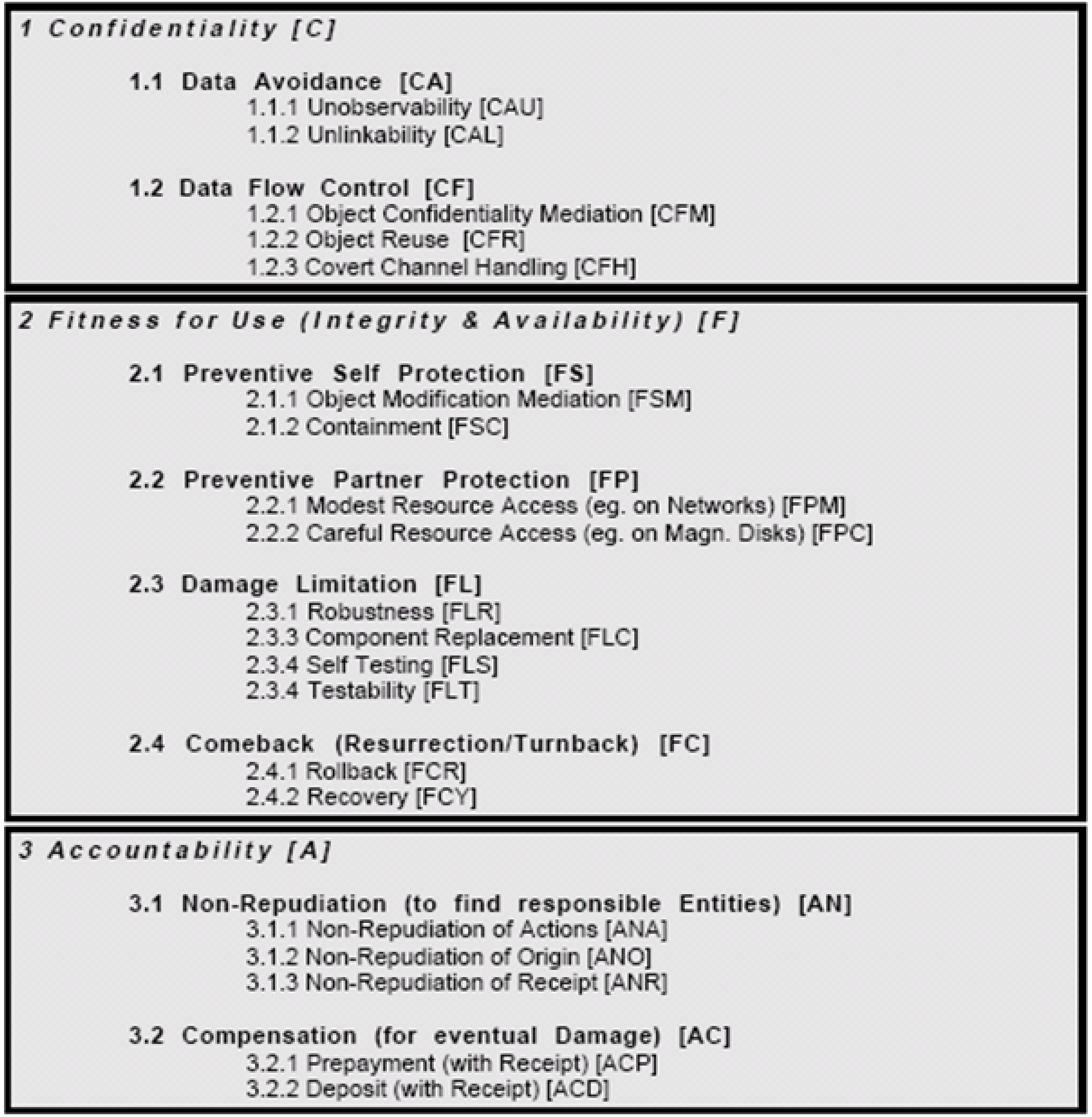
Risk Analysis and Assessment



Risk	Damage	Likelihood	(damage x likelihood)
xx	5000	0.1	500
yy	10	.8	8

Every component is rated along the above dimensions. Damage and likelihood are estimated (which looks rather unsafe at the beginning but turns out to work quite well for practical purposes. As always in security the mere force to make a statement seems to uncover exposures and leads to an improvement already)

Beyond Corporate-Security: Multi-Lateral Sec.



1 Confidentiality [C]

1.1 Data Avoidance [CA]
1.1.1 Unobservability [CAU]
1.1.2 Unlinkability [CAL]

1.2 Data Flow Control [CF]
1.2.1 Object Confidentiality Mediation [CFM]
1.2.2 Object Reuse [CFR]
1.2.3 Covert Channel Handling [CFH]

2 Fitness for Use (Integrity & Availability) [F]

2.1 Preventive Self Protection [FS]
2.1.1 Object Modification Mediation [FSM]
2.1.2 Containment [FSC]

2.2 Preventive Partner Protection [FP]
2.2.1 Modest Resource Access (eg. on Networks) [FPM]
2.2.2 Careful Resource Access (eg. on Magn. Disks) [FPC]

2.3 Damage Limitation [FL]
2.3.1 Robustness [FLR]
2.3.3 Component Replacement [FLC]
2.3.4 Self Testing [FLS]
2.3.4 Testability [FLT]

2.4 Comeback (Resurrection/Turnback) [FC]
2.4.1 Rollback [FCR]
2.4.2 Recovery [FCY]

3 Accountability [A]

3.1 Non-Repudiation (to find responsible Entities) [AN]
3.1.1 Non-Repudiation of Actions [ANA]
3.1.2 Non-Repudiation of Origin [ANO]
3.1.3 Non-Repudiation of Receipt [ANR]

3.2 Compensation (for eventual Damage) [AC]
3.2.1 Prepayment (with Receipt) [ACP]
3.2.2 Deposit (with Receipt) [ACD]

From K.Ronnenberg, Kriterien und Zertifizierung mehrseitiger It-Sicherheit. Note the extension of security to cover ALL participants of interactions. The approach is still limited because it targets IT-Security dangers and not overall risc.

Beyond Corporate-Security: Overall Risc

-EC-Card or credit-card: who carries the risc?

-New bio-security (fingerprints): who gets more security, who less?

-IFF systems in airplanes: who gets safer?

-Police collecting ever more information on citizens. Internally the state organizations lose data and hardware, communicate critical data in an unsafe way, illegally combine date etc.: who gets safer?

-Weapon systems and international treaties: do new weapons make anybody safer? More rich?

-DRM based PCs: who wins, who loses „security“?

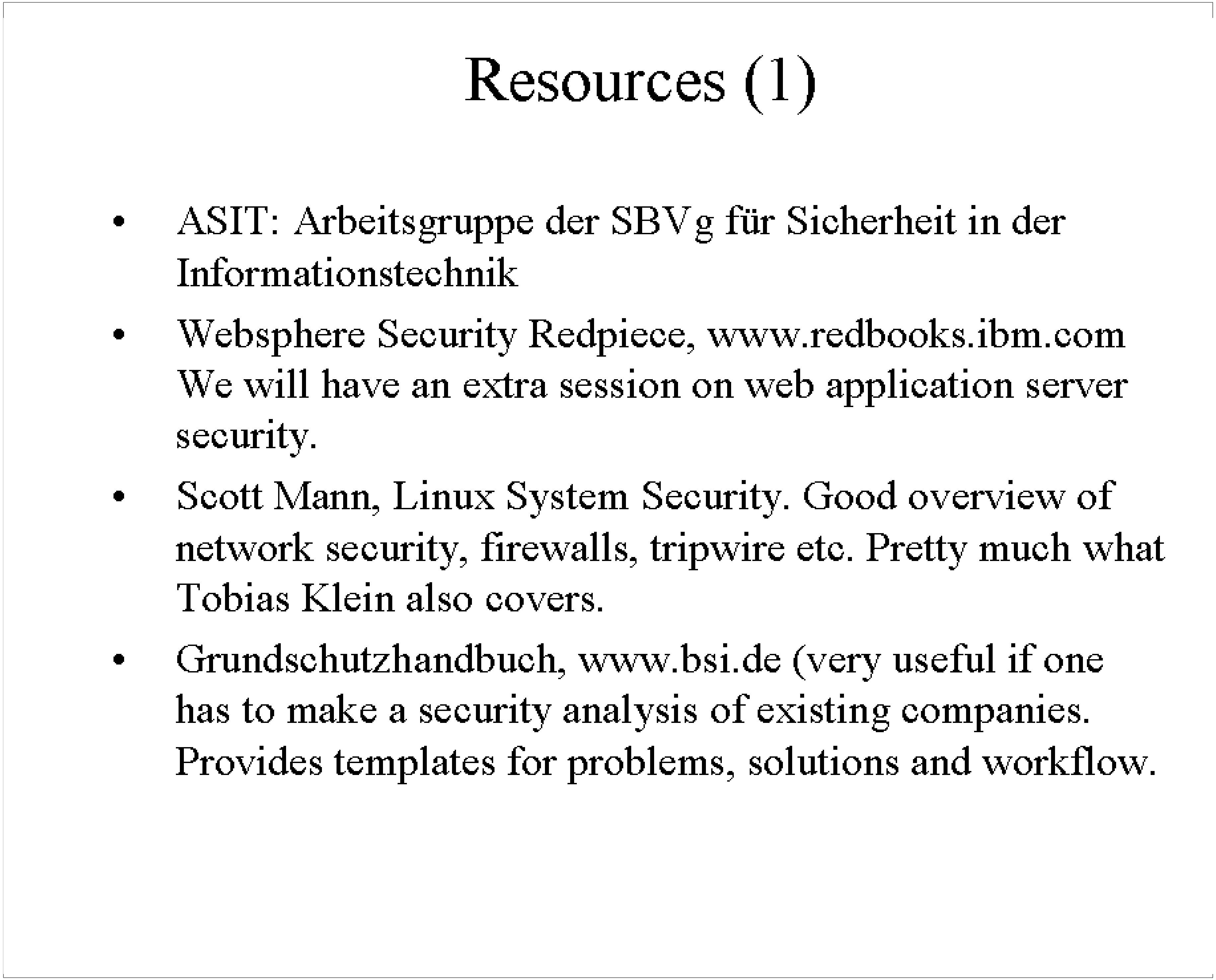
-Vista Security: for MS or the masses?

End-to-end security must not only cover all participants and their right to confidentiality etc. It must also perform a risc analysis for ALL participants from their point of view. This goes deeply into the business and social aspects of security for everybody: When new security technology is rolled out, somebody usually gets better security and somebody frequently less. The DRM example exposes owners to the risc of paying higher prices and less control over things. This is not a „security“ problem per se, but an overall risc problem.

Next Sessions: Firewall Architectures

1. Chances and limits of firewalls
2. IP principles which can be used in firewalls
3. Designing protocols for firewalls
4. Firewall types: routers and application gateways
5. Firwall architectures: from personal firewalls to a large scale DMZ
6. Firewall maintenance (software deployment, logging and auditing)
7. Filtering (ipchains, iptables)
8. Services and Protocols (middleware and specific internet services)
9. An application gateway for SOAP/WebServices

This is pretty much the „canonical“ way to introduce firewalls. Most books on firewalls follow this concept. The services and protocols section is by far the largest but gives a good overview on existing protocols and their problems.



Resources (1)

- ASIT: Arbeitsgruppe der SBVg für Sicherheit in der Informationstechnik
- Websphere Security Redpiece, www.redbooks.ibm.com We will have an extra session on web application server security.
- Scott Mann, Linux System Security. Good overview of network security, firewalls, tripwire etc. Pretty much what Tobias Klein also covers.
- Grundschutzhandbuch, www.bsi.de (very useful if one has to make a security analysis of existing companies. Provides templates for problems, solutions and workflow.