Comprehensive Information Security and

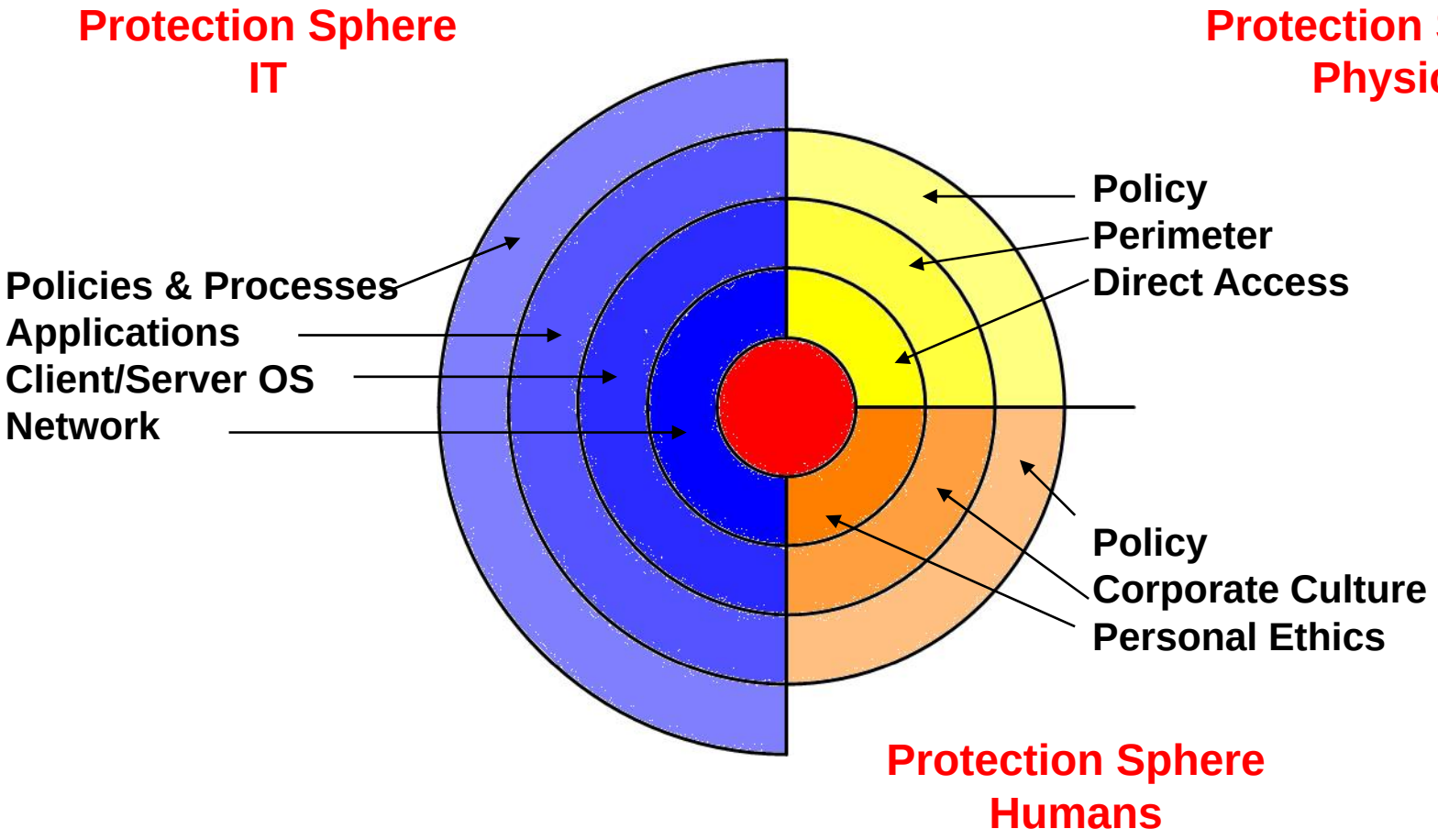
Cyberwar Defence Strategies for Corporations

M. Krausz,
Auditor, Investigator

Comprehensive Information Security

… or „The World‘s a Very Special Onion“

Comprehensive Information Security



Comprehensive Information Security

Examples

- A bank forgets virus protection when migrating from host environment to MS environment

- Telecom: Bad Software + Corporate Arrogance ⇨ Public Security Affair

- University: One server per department per term is simply stolen.

- The Liechtenstein Affair: ⇨ 3 main motives for employees to cause damage: greed, revenge, despair

- Bawag, Soc. Gen., Barings: lack or ineffectiveness of internal controls

- Industry (Defence Sector): Don‘t search for bug three days after initial suspicion

Comprehensive Information Security

What you need to get right …

- Corporate Culture
- Security Department
- Technology & technical processes on five different layers
- Processes (as tight as sensibly necessary or as mandated)
- CISO or CSO must have formal and factual powers
- CISO or CSO is NOT an IT-function. It‘s a business function.

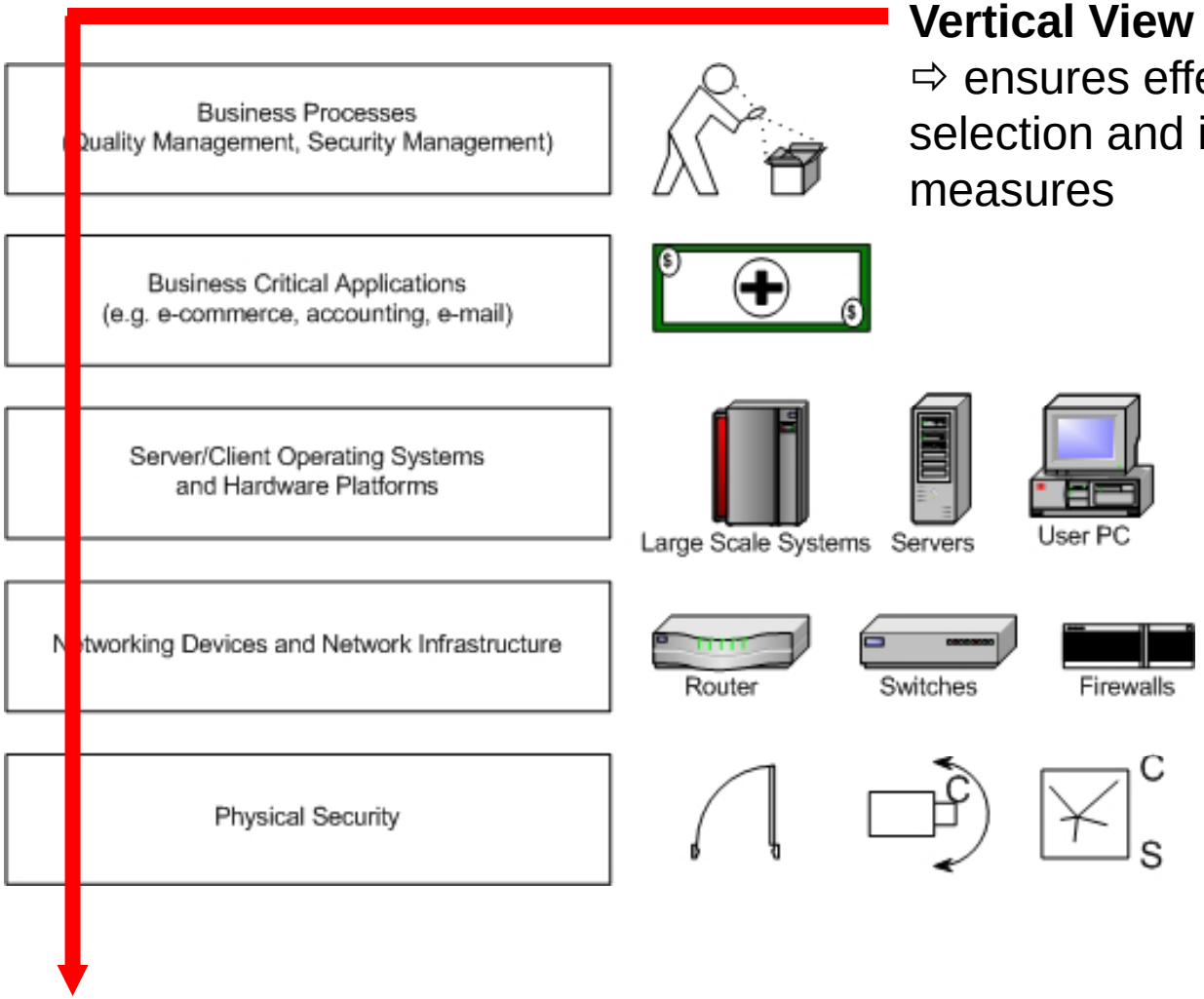
Comprehensive Information Security

Comprehensive Information Security

… or „Vertical is Better Than Horizontal“

Comprehensive Information Security

How to look at things …



Vertical View

⇨ ensures effective and effizient selection and implementation of measures

Cyberwar Defence Strategies for Corporations

Cyberwar Defence Strategies

Are you a likely target for CyberWAR ?

- **Cyberwar**: The usage of IT means and methods in war-like ways to achieve a military or diplomatic goal as part of a political strategy.

- **Affected business branches**:

  - Defence sector
  - Defence sector outsourcing partners
  - Politically exposed companies (or exposed by media coverage)
  - Infrastructure Providers
  - IT (IT-Security) Companies (Reverse Engineering)
  - Collaterally Damaged Companies (e.g. an IP address is attacked, intelligence was bad, a company is hit)

  … all others sequenced by military target priority

Cyberwar Defence Strategies

Defensive Strategies

- Organisational Strategies
- Technical Strategies

Cyberwar Defence Strategies

Defensive Strategies – Organisational Strategies

- Establish and maintain a security department that encompasses the entire organisation. Assure sufficient budget and emergency budget.
- Closely examine your exposure and take business risks only after careful consideration.
- Implement risk treatment before being exposed.
- Maintain a 24x7 alerting structure.
- Establish a working relationship with relevant authorities.
- Share information in peer groups and with CERT‘s.
- Maintain a global internal CERT, if globally active.

Cyberwar Defence Strategies

Defensive Strategies – Technical Strategies

… put simply …

1. **CAPACITY**

2. **MONITORING**

3. **TIGHT APPLICATIONS**

Cyberwar Defence Strategies

Defensive Strategies – Technical Strategies

- Capacity, Capacity, Capacity ⇨ Ensures service levels if under heavy attack

- Security Monitoring (centralized correlation and evaluation of all kinds of relevant logs). Security Monitoring is MORE than IDS and IPS, ranging from detecting unknown devices to access right usage evaluation.

- Implement an appropriate level of redundancy to avoid network and server related single points of failure.

- Keep systems up to date an patched. Use 4-eyes principle for changes. Always verify changes.

- Daring: Make use of non-standard systems

Cyberwar Defence Strategies

Defensive Strategies – Technical Strategies

- If you require high customization of systems ⇨ use open standards and customize/tighten these as much as needed (e.g. Linux as OS)

- Implement operating system hardening for all operating systems used

Contact Information

Michael Krausz
information security consulting

T +43 (1) 253 1000
F +43 (1) 253 1009
M +43 664 301 70 03
mkrausz@i-s-c.co.at
http://www.i-s-c.co.at