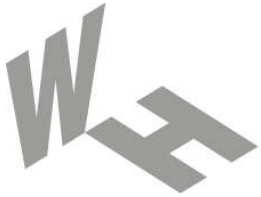


Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Common Approach
→ for more IT security

Prof. Dr. (TU NN)
Norbert Pohlmann

Institute for Internet Security - if(is)
Westphalian University of Applied Sciences
http://www.internet-sicherheit.de

if(is) internet-sicherheit.

Content

- **Internet and IT Security**
  (Situation, problem areas, challenges)
- **Methods for more IT security**
  (Cooperation, sovereignty)
- **The right approach for more IT Security**
  (Analogy, goal orientation)
- **Strategy for more IT Security**
  (Objectives and tasks)
- **Conclusion and outlook**

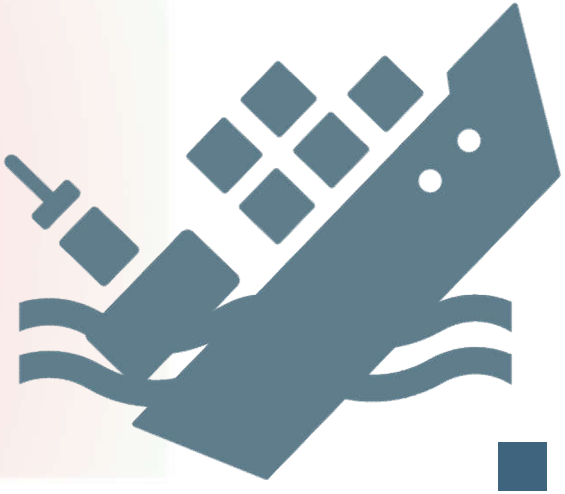
Content

- **Internet and IT Security**
  (Situation, problem areas, challenges)
- **Methods for more IT security**
  (Cooperation, sovereignty)
- **The right approach for more IT Security**
  (Analogy, goal orientation)
- **Strategy for more IT Security**
  (Objectives and tasks)
- **Conclusion and outlook**

Internet and IT Security
→ Situation

- We are currently developing an **Internet society** (source of information, e-commerce, e-government, ..., e-assistant, ..., industry 4.0, the Internet of Things, ...)
- Many local services **are linked to the Internet** (intelligent analysis → Internet connectivity)
- **Private** and **corporate** data stores increase **in the Internet** (central storage → Internet connectivity)

- The IT and IT security technologies are not sure and trustworthy enough!
- Professional **hackers** are very successful!
- The **risk is growing**, the damage too!



What are the problem areas?
→ 1. Privacy and Autonomy

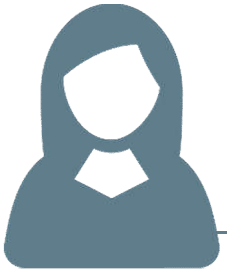
Different perspectives

Cultural differences
(Private data belong to companies? US 76%, DE 22%)

Business models "Payment with personal data"

Privacy / Autonomy

State *(e.g. NSA, BND, ...)*:
Identifying terrorists´ activities?



User: autonomy within the meaning of self-determination

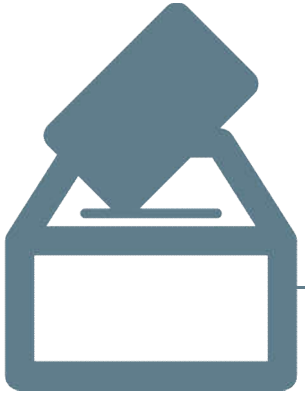
What are the problem areas?
→ 2. Industrial Espionage

about € 51 billion of damage annually

Industrial Espionage

For comparison:
Cybercrime: about € 100 million per year
(Online banking, DDoS, …)

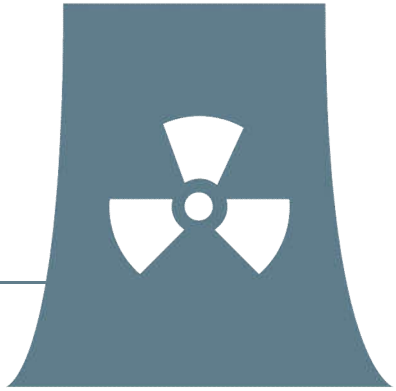
What are the problem areas?
→ 3. Cyberwar



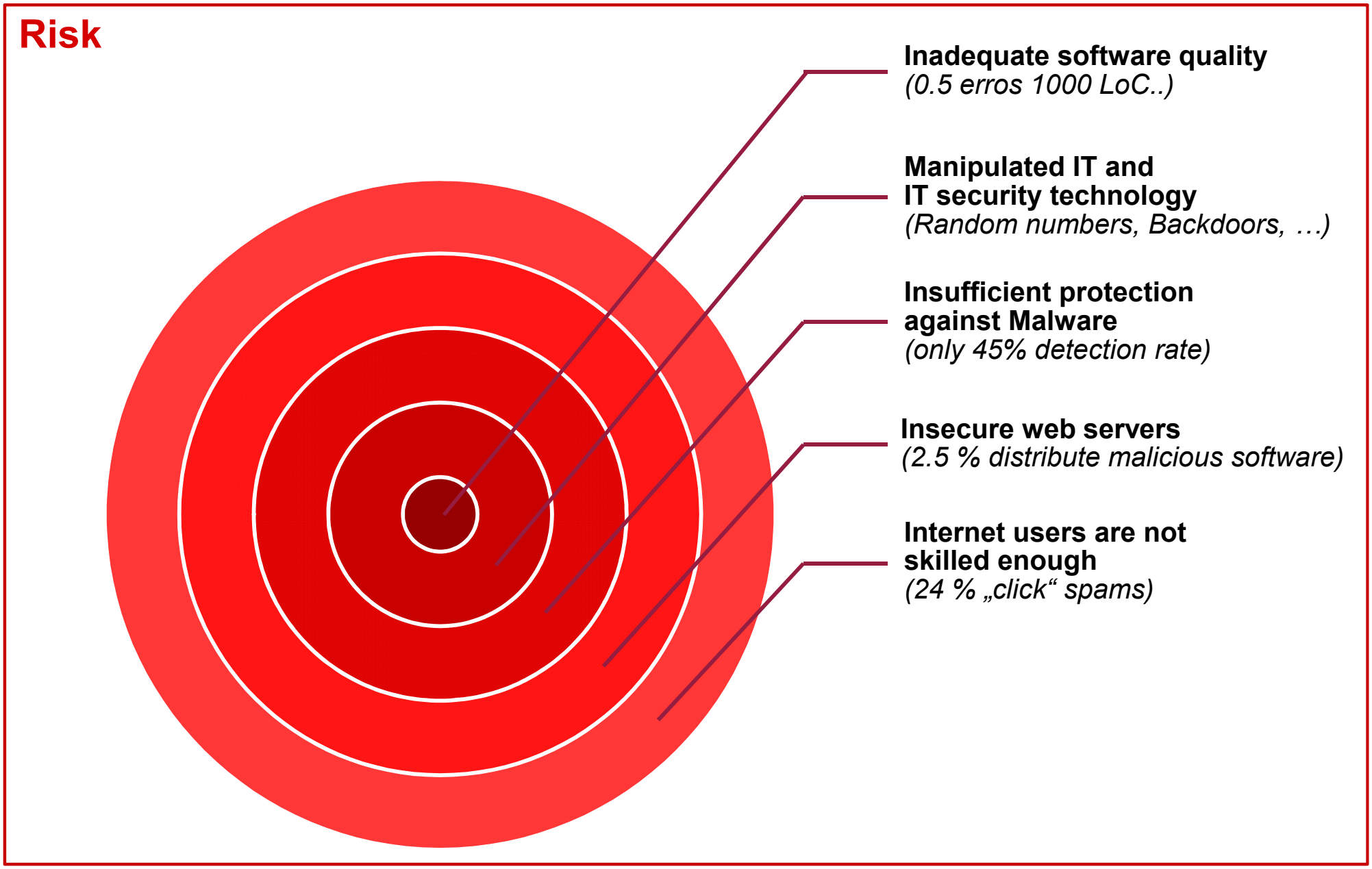
Implementation of policy objectives
→ Simple and “inexpensive”

Cyberwar

Attacks on Critical Infrastructures
e.g. Power supply, water supply, ...



IT Security
→ The biggest challenges



Current Challenges
→ with current risks

- **No** international **identity management**
  (passwords for authentication in the Internet, …)
  - *We **need modern**, easy to use, easy to integrate, … authentication systems, which can be used in every organization (mobile device based, FIDO-ready, different security level, for the **real** and **virtual world**,…).*

www.xign.de

- **New threats** by mobile devices
  (BYOD, quantity instead of quality, tracking, loss / theft, …)
  - *We need intelligent, modern and secure mobile device management systems, which make the use easy for the companies and for the users (**service orientation**)*

- **Too high risks** when communicating
  (e-mail, web, chat, …)
  - *We need modern communication systems, which offer an easy to use, **secure** and **trustworthy communication***

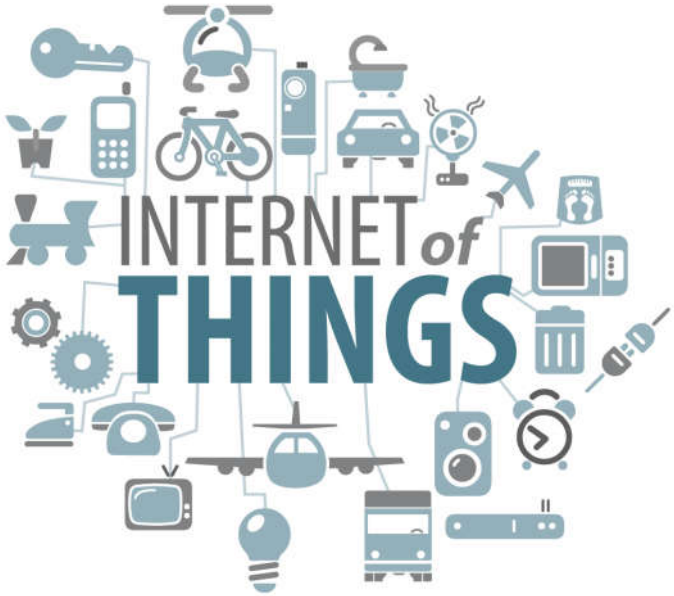
- **Cloud computing** is a major **challenge**
  (session hijacking, place of storage, …)
  - *We need **easy to use**, secure and trustworthy cloud services based in Germany*

...

Current Challenges
→ with future major risks

- **Industry 4.0**
  - Complex systems and control devices are connected to the Internet

- **Internet of Things** (IoT)
  - Nearly all devices in all aspects of life get Internet connectivity



Internet and IT security
→ Evaluation of the situation

- **We know the IT security problems**, but the today available and used IT security systems and IT security measures **do not reduce** the IT security risk sufficiently!

- IT security is a global challenge

- Future attacks **will exceed the current damage**

- **We need innovative approaches** in the field of Internet security to reduce the risk for our society at a **reasonable level**

Current conditions in Europe
→ which will drive the IT security

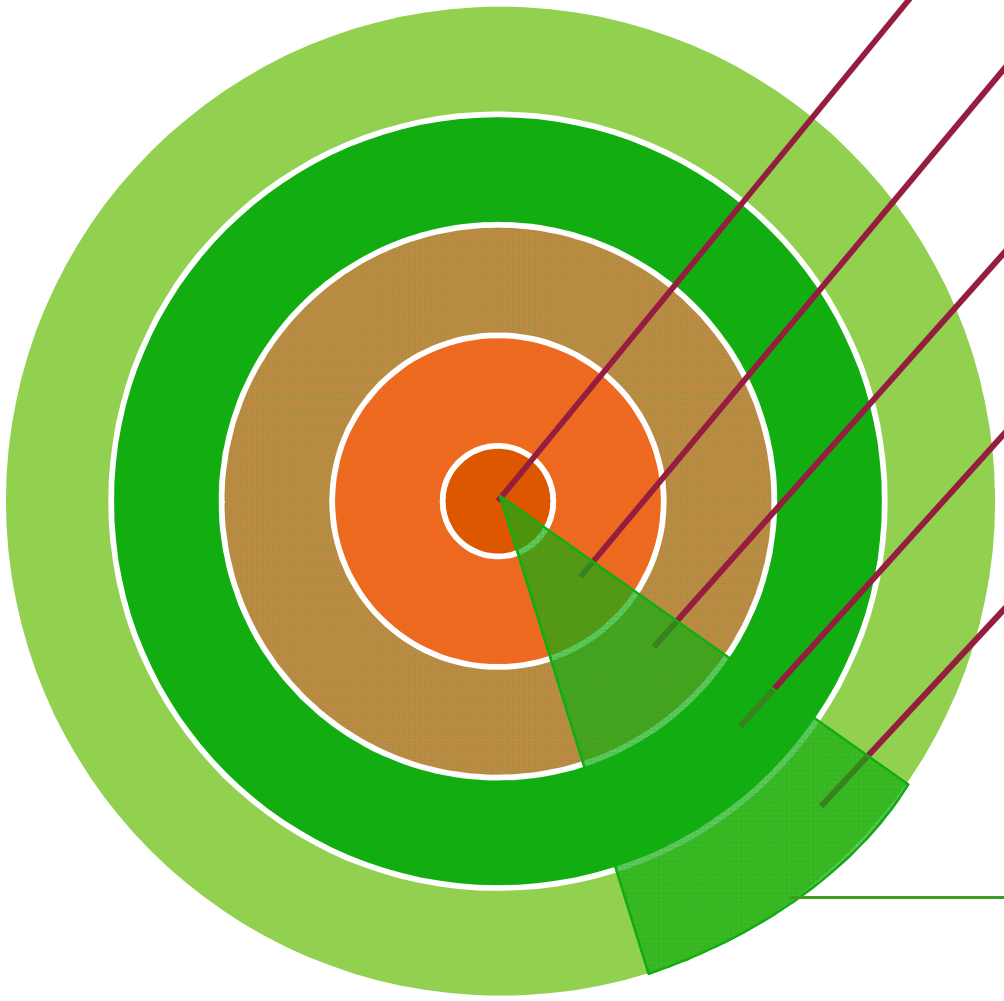
- **eIDAS (European Law for trust services)**
  - Trust Services (→ TeleSec)
    - Electronic Signature (also in the cloud → remote signature)
    - **Electronic Seal** (Signature for organizations)
    - Electronic Time Stamps
    - **Electronic Registered Delivery Services**
    - ...

- **IT security law (in Germany)**
  - **Situation awareness**, SIEM systems, reaction strategies, …
  - Minimum standards, **"State of the art"** and audits will drive the IT security market (critical infrastructure → industry → all user)

Content

- **Internet and IT Security**
  (Situation, problem areas, challenges)
- **Methods for more IT security**
  (Cooperation, sovereignty)
- **The right approach for more IT Security**
  (Analogy, goal orientation)
- **Strategy for more IT Security**
  (Objectives and tasks)
- **Conclusion and outlook**

IT Security Replaceability
→ Standard Software from USA/cooperation



Security Kernel
(Trusted Computing Base)

Isolation, separation and modeling

Modern IT security architecture

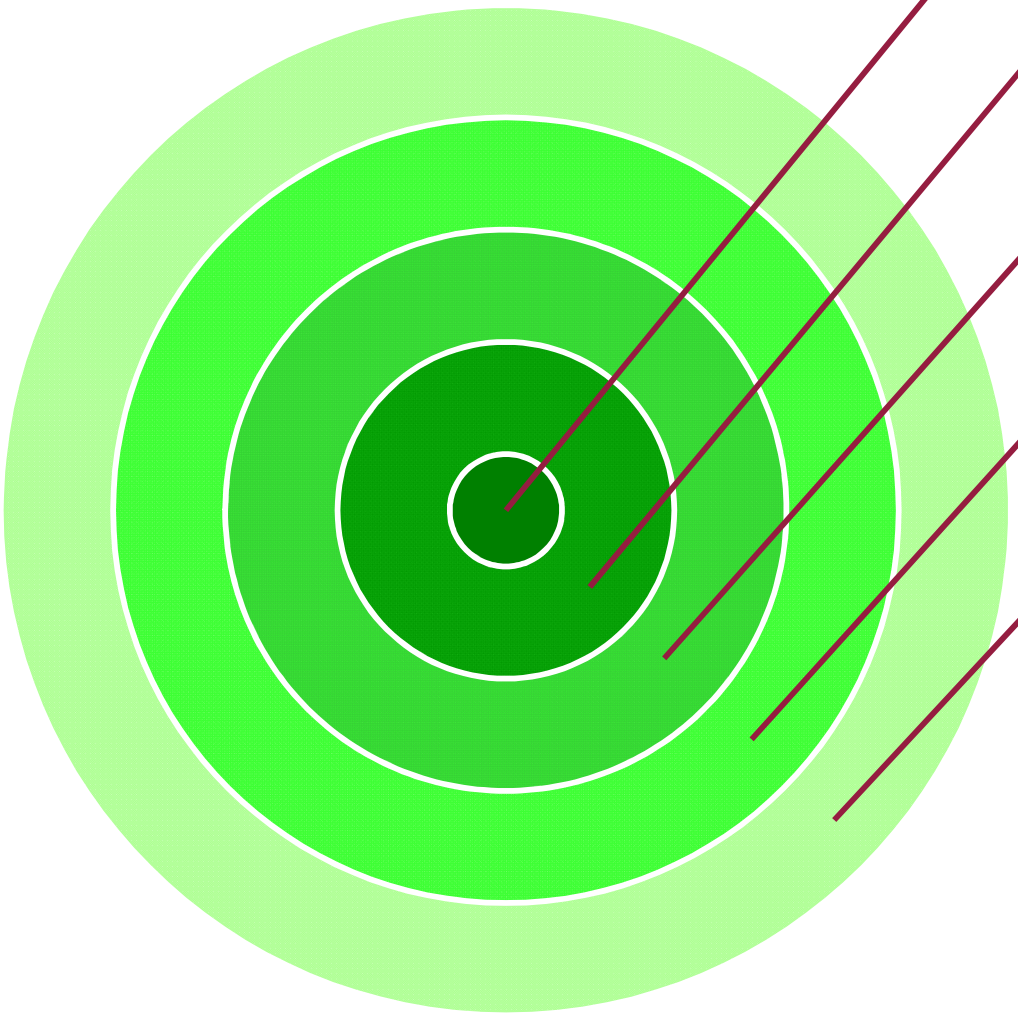
IT Security made in Germany
(no backdoors, no manipulation, …)

More data encryption

Internet users must be well educated

Examples
- **Modern IT security architecture**
- **disk encryption**
- **IP encryption**
- **…**

IT Security Sovereignty
→ Everything comes from DE



Security Kernel
(Trusted Computing Base)

Isolation, separation and modeling

Modern IT security architecture

IT Security made in Germany
(no backdoors, no manipulation, …)

Standardization of interfaces and protocols

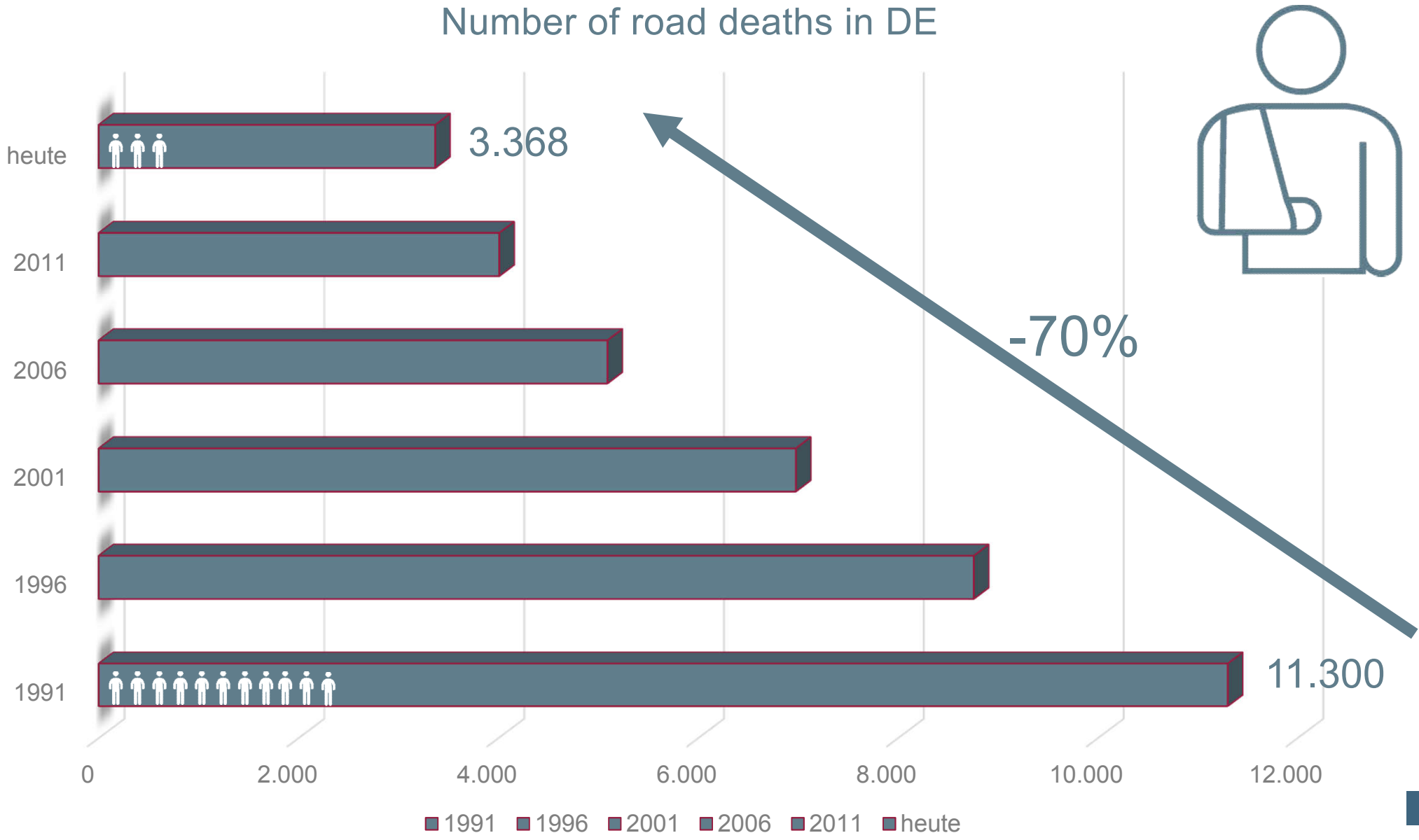
IT security infrastructure

Examples
- **Industry 4.0**
- **Internet of Things**
- **…**

Content

- **Internet and IT Security**
  (Situation, problem areas, challenges)
- **Methods for more IT security**
  (Cooperation, sovereignty)
- **The right approach for more IT Security**
  (Analogy, goal orientation)
- **Strategy for more IT Security**
  (Objectives and tasks)
- **Conclusion and outlook**

Road deaths
→ 1991 until today (analogy)



Quelle: Statistisches Bundesamt/Statista

Rapide reduction of road deaths
→ How was this achieved?

Executive Authorities
("Enforcement", speed limits, traffic regulations)

- ► Seat Belts
- ► Enhanced Drug Tests
- ► TÜV duty for cars
- ► Vests mandatory in case of accidents
- ► Stronger controls of buses and trucks
- ► Awareness car drivers
  (e.g. "Slow Down" campaigns, "seventh sense", ...)

Infrastructure operators
(Cities, states, federal government)

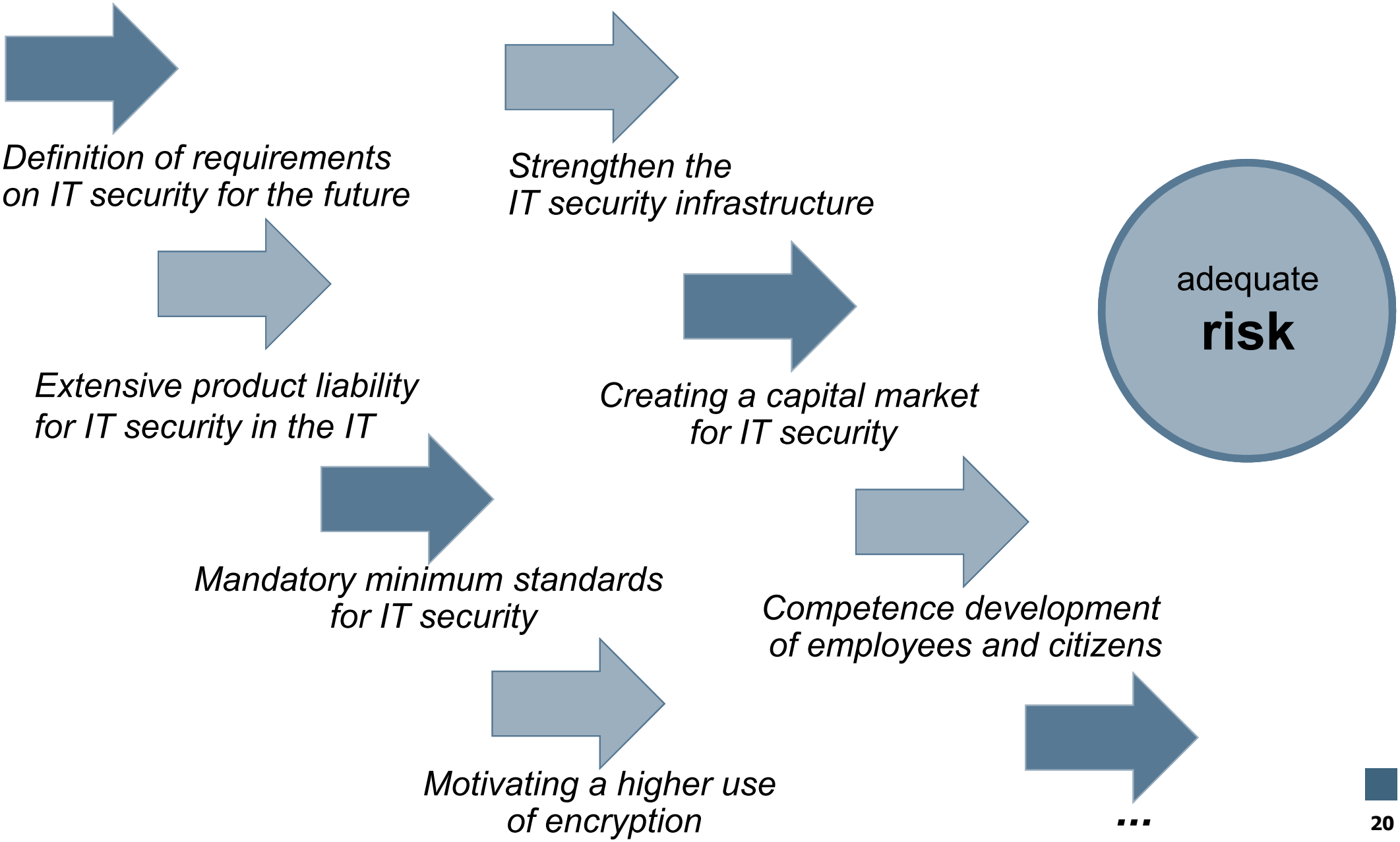
- ► deforested avenue trees
- ► Improved tunnels and bridges
- ► Better infrastructure
  (New streets, modern traffic control systems, , …)
- ► More robust construction
- ► New innovative ideas
  (Car2Car / Communication Infrastructure)
- ► Modern safety systems
  (seat belt, airbag, ABS, ESP, …)

Manufacturers and Suppliers
(Implementation of standards, innovations)

Content

- **Internet and IT Security**
  (Situation, problem areas, challenges)
- **Methods for more IT security**
  (Cooperation, sovereignty)
- **The right approach for more IT Security**
  (Analogy, goal orientation)
- **Strategy for more IT Security**
  (Objectives and tasks)
- **Conclusion and outlook**

Strategy IT Security
→ The general objective and tasks

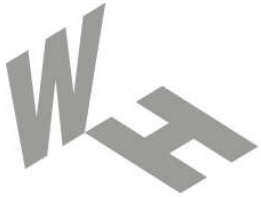


Content

- **Internet and IT Security**
  (Situation, problem areas, challenges)
- **Methods for more IT security**
  (Cooperation, sovereignty)
- **The right approach for more IT Security**
  (Analogy, goal orientation)
- **Strategy for more IT Security**
  (Objectives and tasks)
- **Conclusion and outlook**

Conclusion and outlook
→ focused and common activities

- We now have to define common objectives **with all stakeholders** and actively implement tasks accordingly!
- **IT security manufacturers**
  *(Simple, manageable and **combined solutions** that are well integrated in technologies, products and services, ...)*
- **User Companies**
  *(**purchasing cooperatives** in order to motivate for example modern IT security architectures, existing and needed solutions have to be used actively, ...)*
- **Universities**
  (Close gaps, meet new requirements, generate innovation in the necessary fields, ...)
- **State**
  (Motivation of the necessary steps and promotion / regulation, …)
- **User**
  (Demand new business models, obtain skills, …)



Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Common Approach
→ for more IT security

The right way to
a trusted and secure modern future

Prof. Dr. (TU NN)
Norbert Pohlmann

Institute for Internet Security - if(is)
Westphalian University of Applied Sciences
http://www.internet-sicherheit.de

if(is)
internet-sicherheit.