

# Building trust in digital business and driving the security industry



**Chairman:**  
**Dr. Hans-Joachim Popp**  
German Space Agency



**Chairman:**  
**Dr. Rolf Reinema**  
Siemens

## What we have found!

The key conclusions from the session:

- Economy based on Digital Communication needs profound changes in the way, relationships are maintained. More connections need more interfaces which increases the urgency
- Security Management will have to change towards Risk Management over time
- The “golden nuggets” have to be redefined while value of information changes dramatically with evolving technology, maturity of new business and crime models
- Data volumes of high risk business data (customers persona data, transaction data etc.) are rising, so does the need to protect them against sophisticated threats
- Building trust needs a transparent relationship over time.
- Software quality measures and security by design concept will be needed to enhance the overall risk situation
- Not only data theft but data manipulation will be a future threat for all businesses (since all will be based on digital systems).

## What we have explored

Among these conclusions, we have developed one of these in greater detail below:

### 1. How is trust between partners being developed and fostered?

- Successful new business models have developed reputation models
- The question will be: who owns the authority needed for the model to be effective?
- There will be (as in real live) different levels of trust according to the value of the relationship driven on a certain communication.
- New European Code of Conduct, authorities that are able to check the behavior of participants.

### 2. What changes are necessary in risk treatment

- Location of data storage => Definition and enforcement of data access rules
- Plug & Play => Transparent communication
- Data storage based on risk status

### 3. Management of Sec. Incidents

- New legal notion system & new technical solutions
- Exchange of threat information

## What we have left open...

Mobile Device Management: must have ?

- **We had a common understanding that a new ethical framework for digital business has to be created. The rules for this remain to be set up.**
- **Detection of Threats will become extremely difficult. Technical and organizational solutions have to be found.**

## Convergences

What points do we share in common:

- › Modification of legal framework urgently necessary
- › Standards necessary, but not to be enforced (except for sec technology missing)
- › Classification of crucial data elements urgent in order to cope with volumes in a meaningful way

## Differences

What points do we agree to disagree:

- › Open Source Software was not agreed to be a crucial driver for enhancing transparency, some of us see it inevitable to deal with it
- › Having more players in the market of standard basic tools (DB, OS etc,) where not common sense

## A picture is worth a thousand words

An illustration that sums up our results:

### Adopting Modern Security Methods Step by Step



"I DON'T THINK YOU UNDERSTAND THE CONCEPT OF CYBERSECURITY."