Connect Germany

GTUG

GO INTERNATIONAL

(25), 26, 27 September 2012
Conference & Exhibition
at The Westin Bellevue Dresden, Germany

Security Workshop

Dresden, Sep 25th, 2012

CSP Computer Security Products Inc.

Thomas Leeb

greenHouse Software & Consulting

Carl Weber

bank-verlag

Wolfgang Breidbach

CSP Security.com
SOLUTIONS FOR HP NONSTOP SERVERS

IT Security to achieve Compliance - or vice versa ?

Thomas Leeb

Executive V.P. – Global Sales

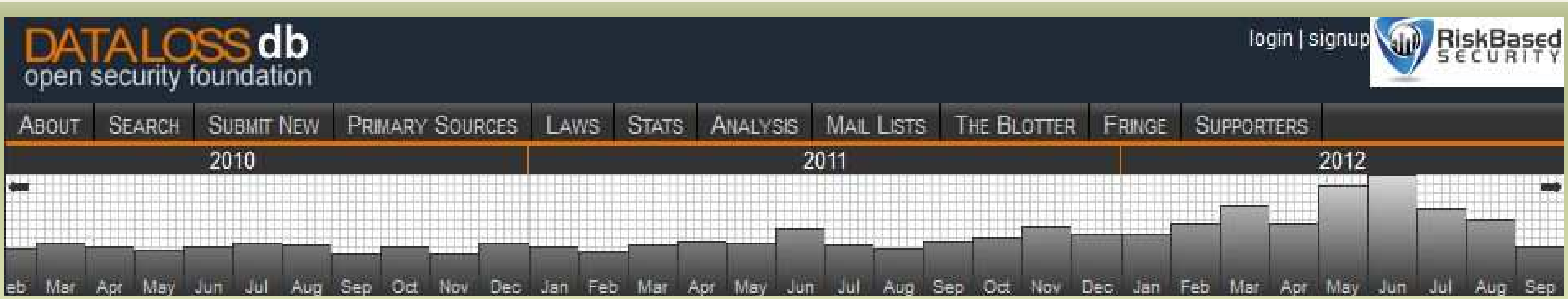
WWW.CSPSECURITY.COM

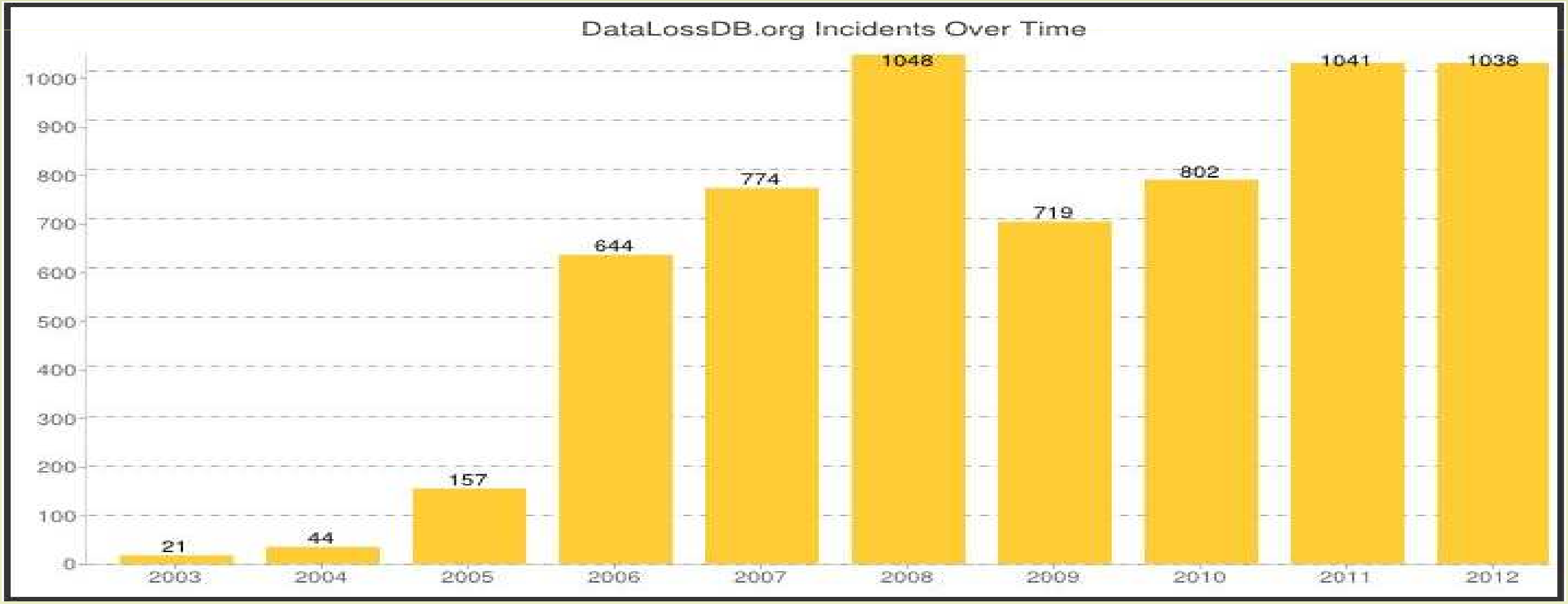
GTUG Hotspot 2012, Dresden, Sep 25th, 2012

About CSP

- Based in Toronto, Canada.
- Security and Audit Solutions for Enterprises.
- Leading Provider of Security Solutions for the HP Nonstop market.
- Growing customer base
- Cross Platform Security Management
- Customers include:
  - Largest Banks
  - Payment Processors
  - Major Stock Exchanges
  - Defense and Healthcare organizations
  - Telecommunications
  - Manufacturers

Average : 2 data breaches every day

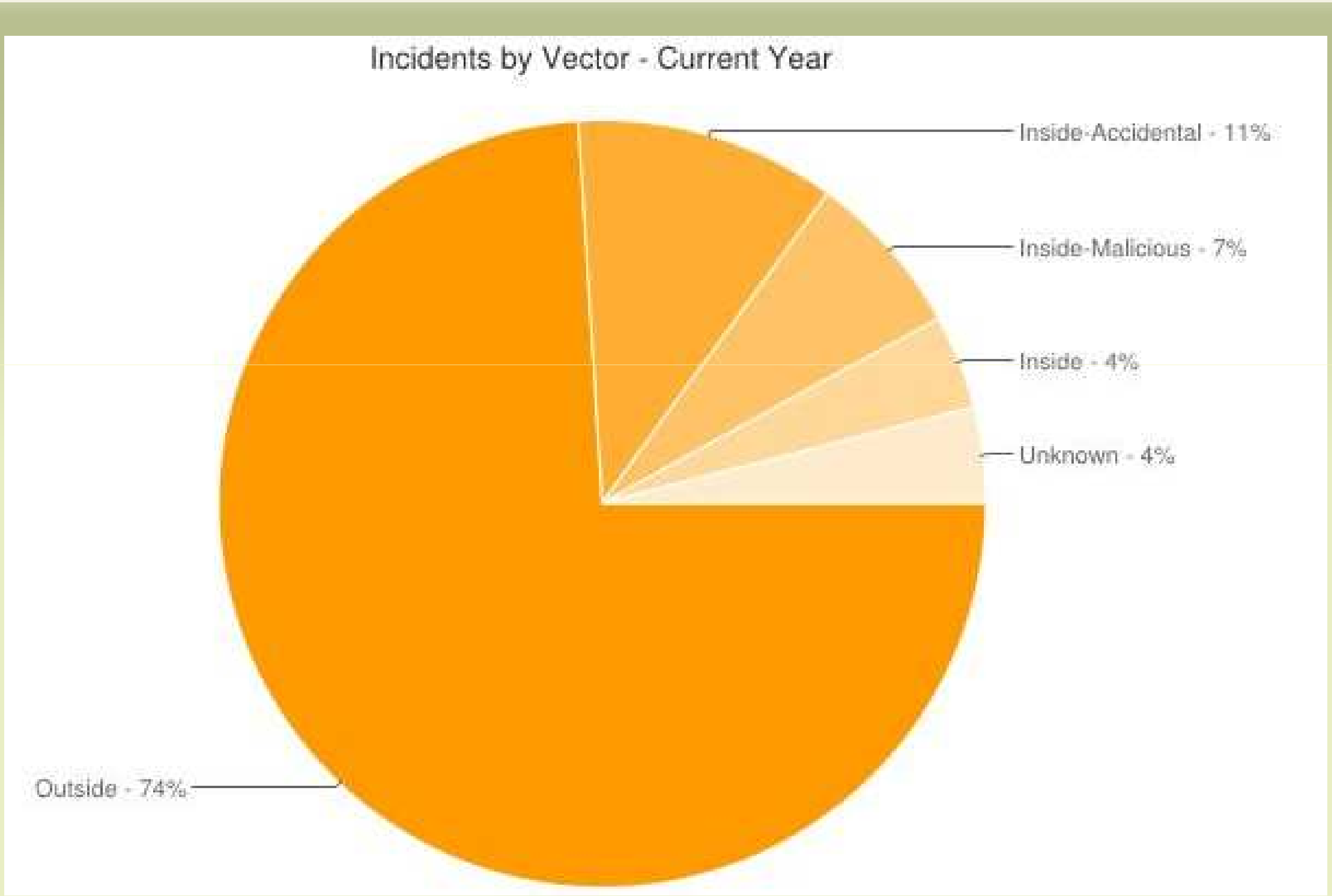




Source : DataLossDB.org

CSP | CSP Security.com
SOLUTIONS FOR HP NONSTOP SERVERS

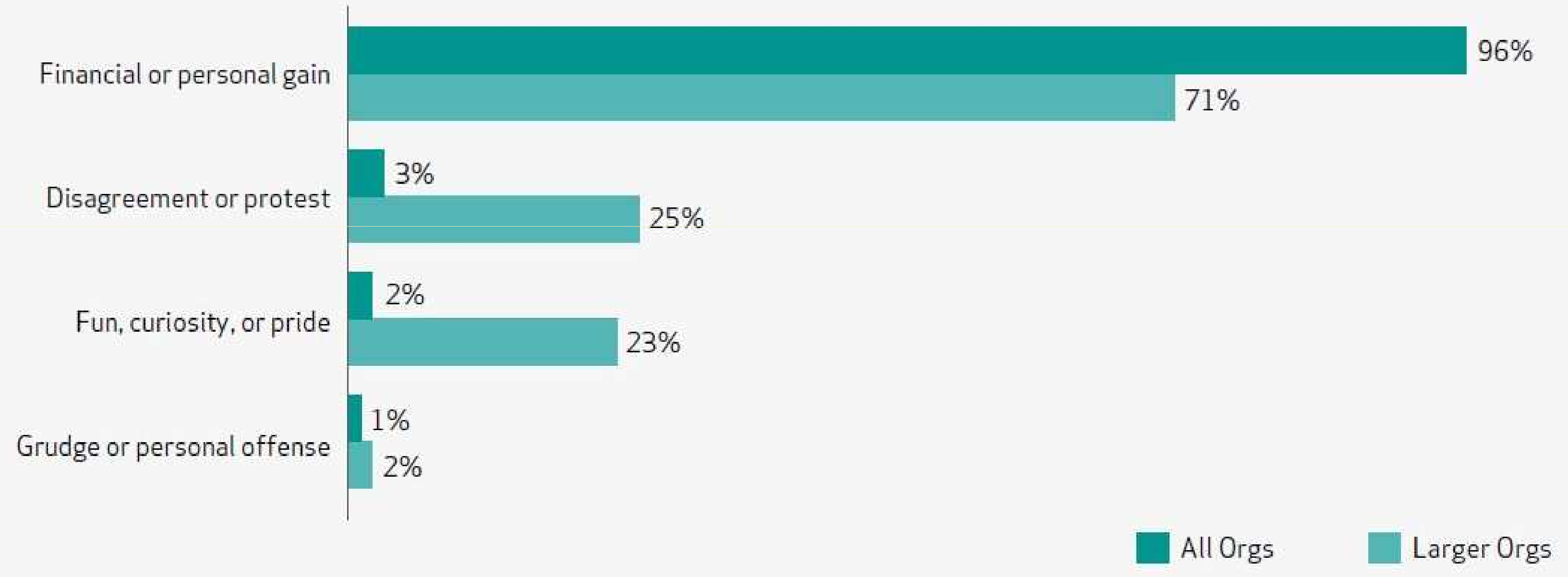
Attacks from outside dominating and increasing



Source : DatalossDB.org 2012

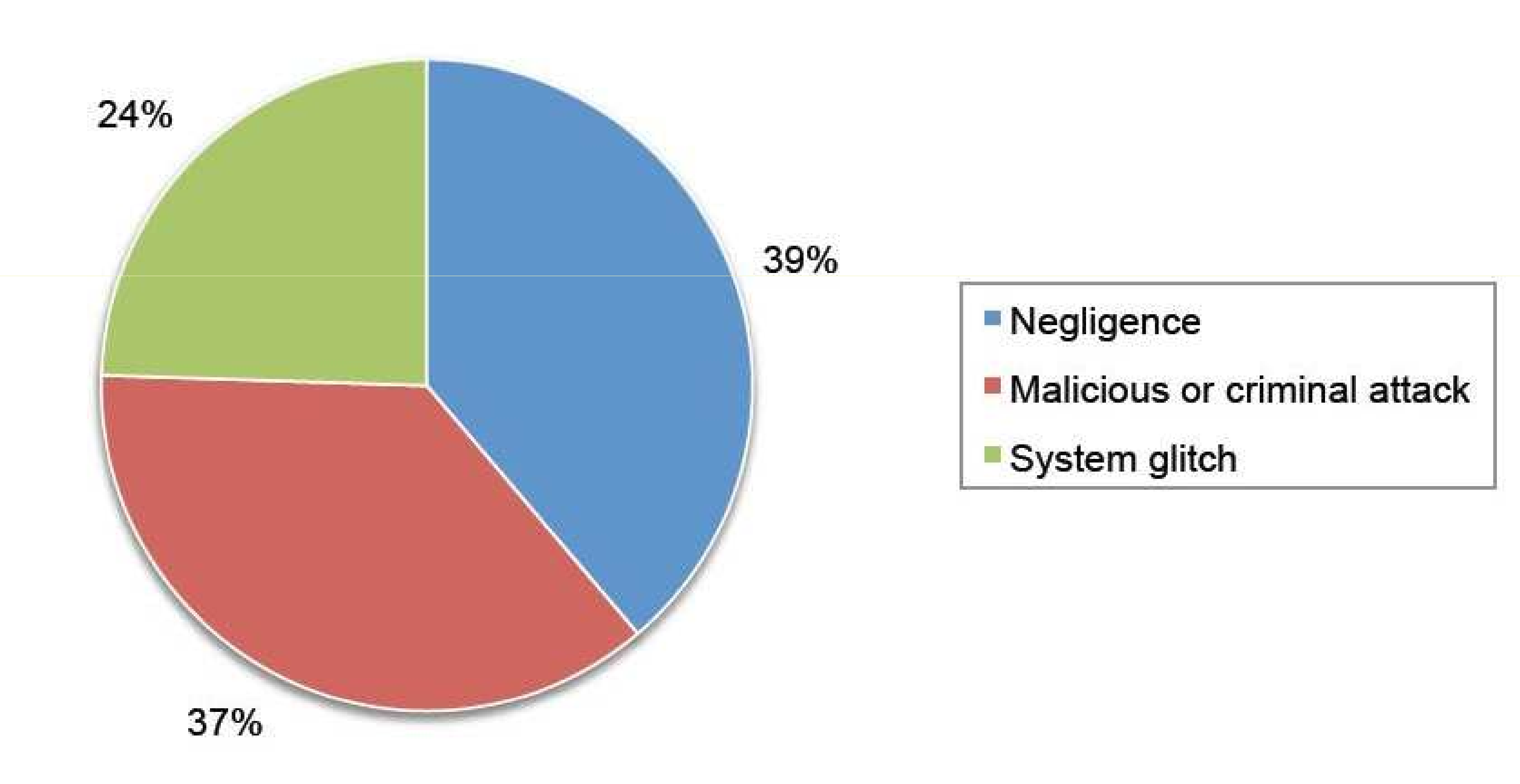
The Motivation for Cyber Criminals

Figure 15. Motive of external agents by percent of breaches within external



Source : Verizon 2012

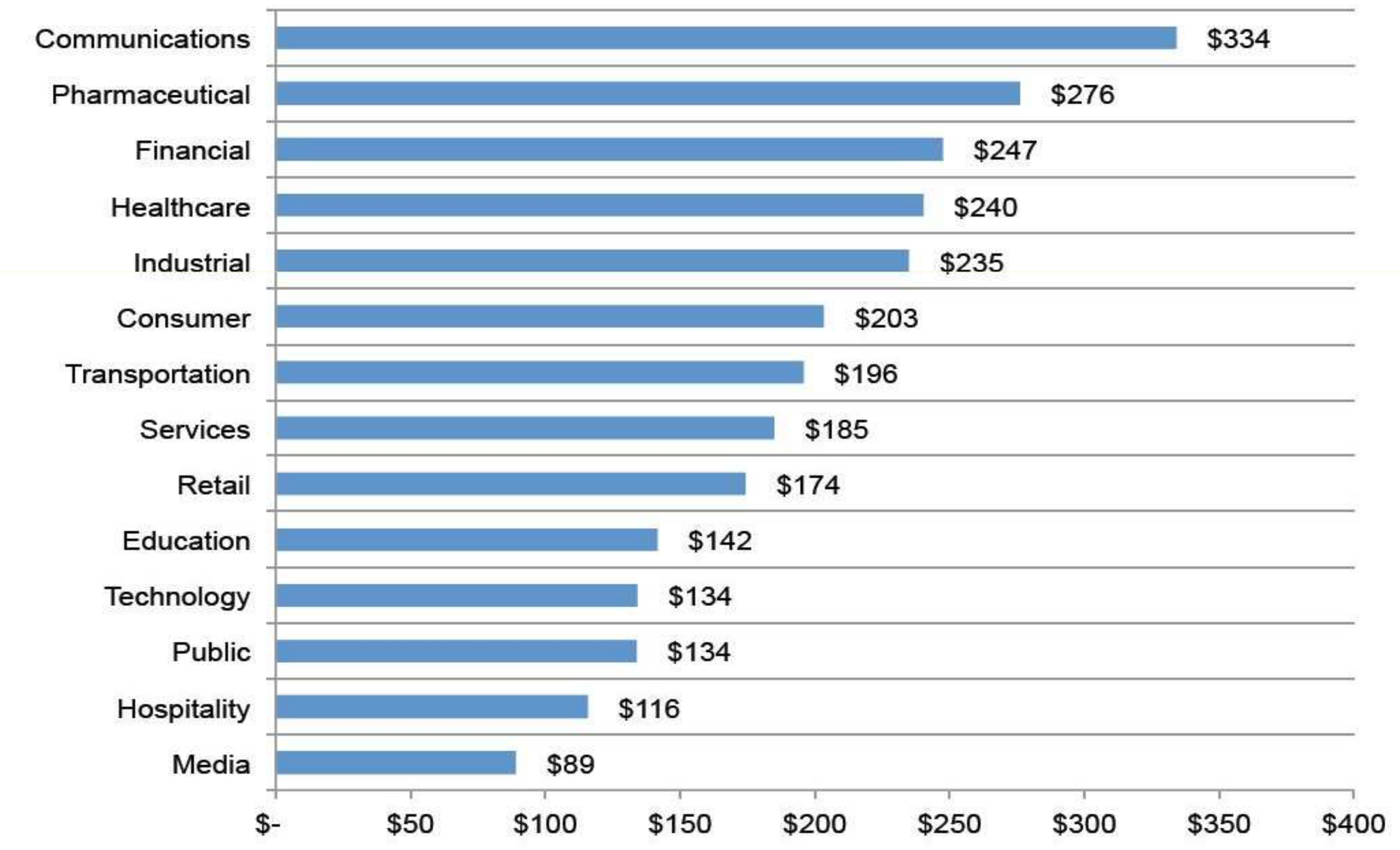
Root Cause of Breaches



Source : Ponemon Institute 2012

Costs resulting from breaches by Industry

Figure 4. Per capita cost by industry classification of benchmarked companies



Source : Ponemon Institute 2012

Sample victims – payment card industry

- Merchants
  - TJX, 2007
    - Tier 1 (>6M tx/month)
    - Intrusion detected 1,5 years after intrusion
    - 94M card details exposed
    - 150$ reported costs
  - Hannaford, Mar 2008
    - 4,2 M cardholder details
- Payment Processors
  - RBS Worldpay, Dec 2008
    - 1,5M cardholder details
    - Coordinated attack – ATM heist 9M$
  - Heartland , Jan 2009
    - >100Mtx/month
    - > 250k merchants, about 1000 banks – affected 673 banks, 130M cardholders
    - Intrusion occured 8 months beforedetection
  - Global Payments, Apr 2012
    - 1,5M credit/debit card details potentially compromised
    - Est cost 114M$

PCI DSS – some observations

Source : Computerworld (related to Hearing at US House of Representatives)

- „Done little to stop payment card data thefts“
- „the standard is clearly not enough to protect cardholder data“
- Hannaford
  - certified just one day after they were informed about the system intrusions.
  - received PCI certification while intrusion was in process.
- RBS Worldpay and Heartland were both certified prior breaches.
- Voices of US retailers :
  - „Card issuers are requesting us to store card data. When a breach happens, we are the ones who bear the costs and who are demonized.“
  - „PCI has been developed from the perspective of card companies as opposed to from that of those who are epected to follow them.“
  - „PCI is little more than a tool to shift financial risks off card companies and banks. We are forced to spend billions to implement a standard, which has done little to improve security.“

PCI DSS – observations (cont)

Source : Computerworld (related to Hearing at US House of Representatives)

- PCI SSC : „breached organisations were not „compliant“ at the time of the breach.“
- VISA :
  - „The ‚Heartland case‘ never should have happened and is unfortunate, but this does not make me question the tools.“
  - „However it‘s time for security controls to go beyond what‘s included in PCI now
- VISA working with banks and retailers to test new security measures
- New degree of uncertainty about the future of PCI specifications
- Growing chorus of doubt about effectiveness of PCI

Learnings from the sample „PCI Compliance“

- Procedural weaknesses
  - Consequences of non-compliance vs. Consequences of breach
  - Compliance certificate
    - How do I get it ?
    - How do I lose it ?
  - QSA („the neutral advisor and policeman“)
    - From assessment to final audit
    - From assessment report, recommendations to solutions
- What it isn‘t :
  - Platform specific (i.e. HP Nonstop File system, Pathway, Spooler, TMF)
    - Unique advantages causing unique challenges
  - A complete guideline for security measures
    - Would the QSA spot everything requiring improvement ?
    - Are we aware about weaknesses outside the assessment report ?
    - How do we deal with them ?
- What it is :
  - mandatory

A Risk Managed Approach to Security

- What could go wrong ?
- What‘s the probability of it happening ?
- What would be the consequences ?
- How can we reduce the probability of it happening ?
- How can we reduce the impact if it did occur ?
- How will we know that it is occuring or about to occur ?
- What is our contingency plan if it does occur ?

Security Policies

•Procedures

•employees

•contractors

•visitors

•IT security

•Audit/Compliance

•Authentication

•Password Quality

•Data Encryption

•Command Control

•Access Control

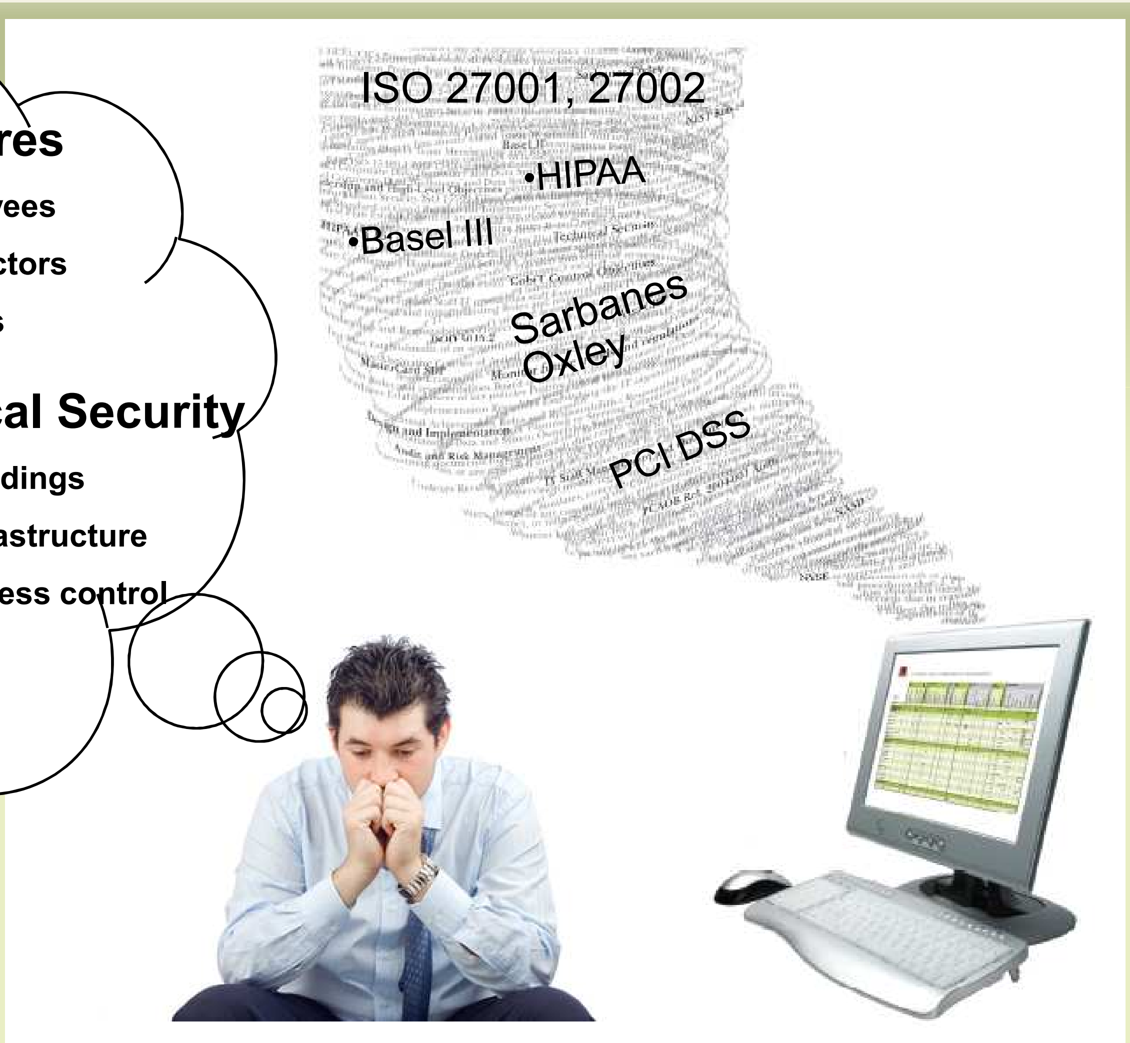
•. Etc.

•Physical Security

•Buildings

•Infrastructure

•Access control



Conclusions – part 1

- **Compliance programs are**
  - Important to set common standards
  - great if used as integral part of the risk management process
  - useless if (ab)used as strategic security initiative
- **ISMS to ensure**
  - Consolidated View of Security Requirements
  - Link with Enterprise Risk Management
  - Continuous Improvement Cycle (Standards not evolving quickly enough)
  - Awareness and Culture for Enterprise Data Security
- **Reduce Risk (Probability x Potential Impact)**

CSP Security.com
SOLUTIONS FOR HP NONSTOP SERVERS

Thank you !

**„Distrust and Caution
are the parents of Security.“**

(Benjamin Franklin)

For additional information please contact

Thomas Leeb (CSP EMEA)
thomasl@CSPsecurity.com
+43 699 1856 3888