CSP | CSP Security.com
SOLUTIONS FOR HP NONSTOP SERVERS

Compliance is not enough

Thomas Leeb

Director Business Development
CSP EMEA

CSP
WWW.CSPSECURITY.COM

VNUG 2010, Gällöfsta Manor, May 27th, 2010

About CSP

- Based in Toronto, Canada.
- NonStop® DSPP Partner since 1987.
- Develop, Support and Distribute Security and Audit Solutions for the HP NonStop® Market.
- Over 250 Customers and over 1000+ licenses World Wide
- Customers include:
  - Largest Banks
  - Major Stock Exchanges
  - Defense and Healthcare organizations
  - Telecommunications
  - Manufacturers

Business Partner
hp invent

Integrity Ready Partner
hp invent

Agenda / Why should you care ?

- Data breaches and resulting costs still increasing
- PCI DSS
  - Has it really helped to improve security ?
  - What are observations and learnings so far ?
  - Lessons from the „Heartland“ case
- Approaching Security
  - Security = minimise risk = decrease probability * decrease impact
  - So how to approach it, and how to deal with PCI DSS then ?
  - Establishing a solid ISMS
- CSP and how to address the 2 dimensions

Costs resulting from Data Breaches

Source : Ponemon Institute (Study 2009)

- Overall Costs continue to rise
- Study 2009 : 45 US organisations from 15 different industry sectors
- Avg. Costs per organisation: 6,75M$ (204 US$ / rec)
- Largest case 101.000 records – 31 M$ in breach related costs (or 307 US$ / rec)
- increasing focus on implementing automated IT-security solutions
  - Identity and access management solutions
  - Expanded use of encryption
  - Dataloss prevention solutions
  - Endpoint security solutions
- Data breaches from malicious attacked doubled from 2008 to 2009
  - „data-stealing“ malware increasing
- Organisational Leadership
  - Companies without CISO (or similar) experience 50% higher costs

Mar, 2008 : Hannaford – Data breach affected millions of shoppers

Source : Computerworld

- Intrusion into computer network of supermarket chain (Maine, US)
- Forced banks to reissue millions of credit and debit cards
- MBA reported 70 of its member banks were contacted by Visa, MC
- 4.2M Credit & debit card numbers stolen during transmission
- Included data from magnetic stripe
- Hannaford instructed consumers to check their card statements
- Felt they met and in many cases exceed industry standards on security measures
- Now „committed to take whatever steps may be necessary“ to enhance security

Dec 23rd, 2008 - RBS Worldpay Data breach resulting in ATM heist – 9M$ stolen

Source : Computerworld

- Hackers broke into database to get personal data
- 1.5 M cardholders affected
- Social security numbers of 1.1M individuals may have been accessed
- Information included financial data on payroll cards
- Personal information „may“ have been affected

- Feb 6th : coordinated attack on Nov 8th by „cashers“ withdrawing 9M$ using counterfeit cards on 130 ATMs, in 49 cities, within 30 minutes
- Hackers able to mess with card limits ? (100 cards)
- FBI spokesman : „People are out there attacking computers every day, but this one is different in scope, timing and coordination of the attack.“

Jan 20, 2009 : Heartland – Card processor victim of largest data breach

Source : Computerworld

- Visa, MC alerted about suspicious transaction activity, Heartland found evidence of malicious software compromising data
- Forensic exams has shown multiple instances across their network
- Processing >100M tx/mth for >250k merchants and hundrets of banks
- Included card numbers, exp and Track-2 data
- Dropped from PCI compliance by Visa
- Gartner :
  - „Cybercrooks are increasingly targetting payment processors. Attacking processors much more serious than retailers“
  - „More radical moves required, PCI is clearly not enough“
- Feb 13th : over 440 financial institutes affected in 40 U.S. states, Canada and outside, lawsuits ongoing – meanwhile corrected to 673
- May 2009 : Intrusion occured in May 2008, not detected until Jan
- Oct 5th, 09 : breach believed to have started in Dec 2007 already

PCI DSS – some observations

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

- „PCI DSS has 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 progess.
- 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 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.“

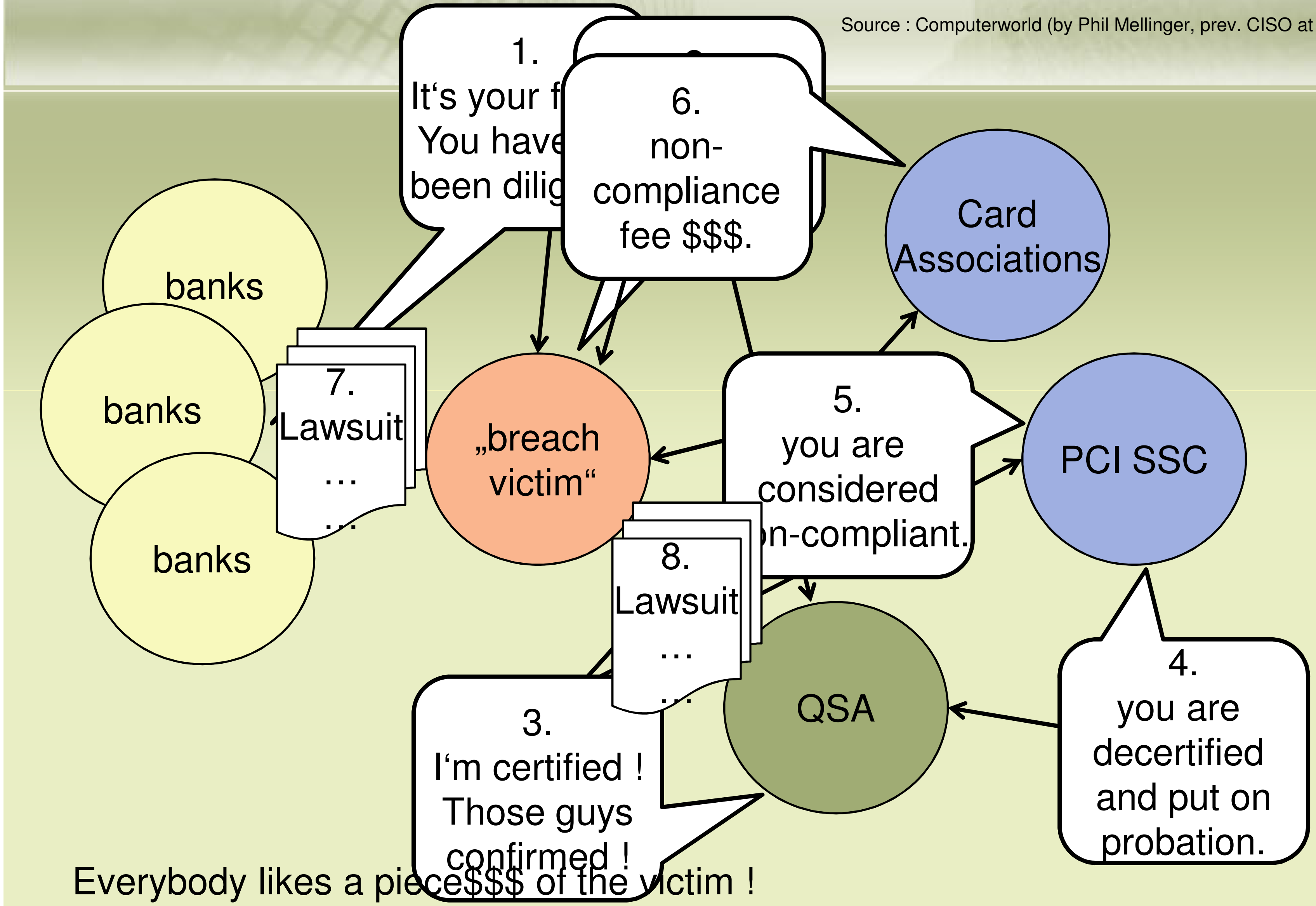
PCI DSS – observations (cont)

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

The PCI Blame Game

Source : Computerworld (by Phil Mellinger, prev. CISO at First Data)



Everybody likes a piece$$$ of the victim !

Prepare for the „third“ attack wave

Source : Computerworld (by Phil Mellinger, prev. CISO at First Data)

- Phase 1 (1990‘s)
  - first cyber attack wave aiming at Internet merchant databases
- Phase 2
  - PCI DSS was introduced post millenium,
  - hackers already „hooked on“ cash and updating their weapons
  - If stores would no longer store card data, attackers would use sniffing technology to read them while in transit
  - Breach-funded attackers improved their skills to yet unknown levels
- Phase 3 (2005 – now)
  - trojans became invisible to firewalls, AV tools
  - Botnet controllers scaled up to manage massive numbers of infected PCs
  - Key-logging techniques perfected to collect valuable browser input
  - Undetectable trojans organised into huge botnets efficiently collecting data
  - Targets increasingly online financial institutions
  - Attackers quickly morph trojans to new and yet again undetectable variants
  - Russian cyber attackers meanwhile outsource cyber-attacks to China

What can be done ?

Source : Computerworld (by Phil Mellinger, prev. CISO at First Data)

- Stop the blame game
  - infights, litigation, fines over breach responsibility is not useful
  - Reward the ones in the industry, who identify weaknesses rather than punish the attack victims
- PCI rules must evolve to address „3rd wave“ attacks
- Improve fraud intelligence to understand attackers and their weapons
  - „No longer sufficient to monitor internet chat rooms“
  - Now the task is to infiltrate the attackers
- International laws
  - If domestic law enforcements are not dealing with the attackers operating within their borders, create ability to hold those countries accountable
  - Countries, who „protect“ cyber-attackers are no different than those providing safe heavens for terrorists
- New security approaches and tools required to thwart attacker‘s weapons.

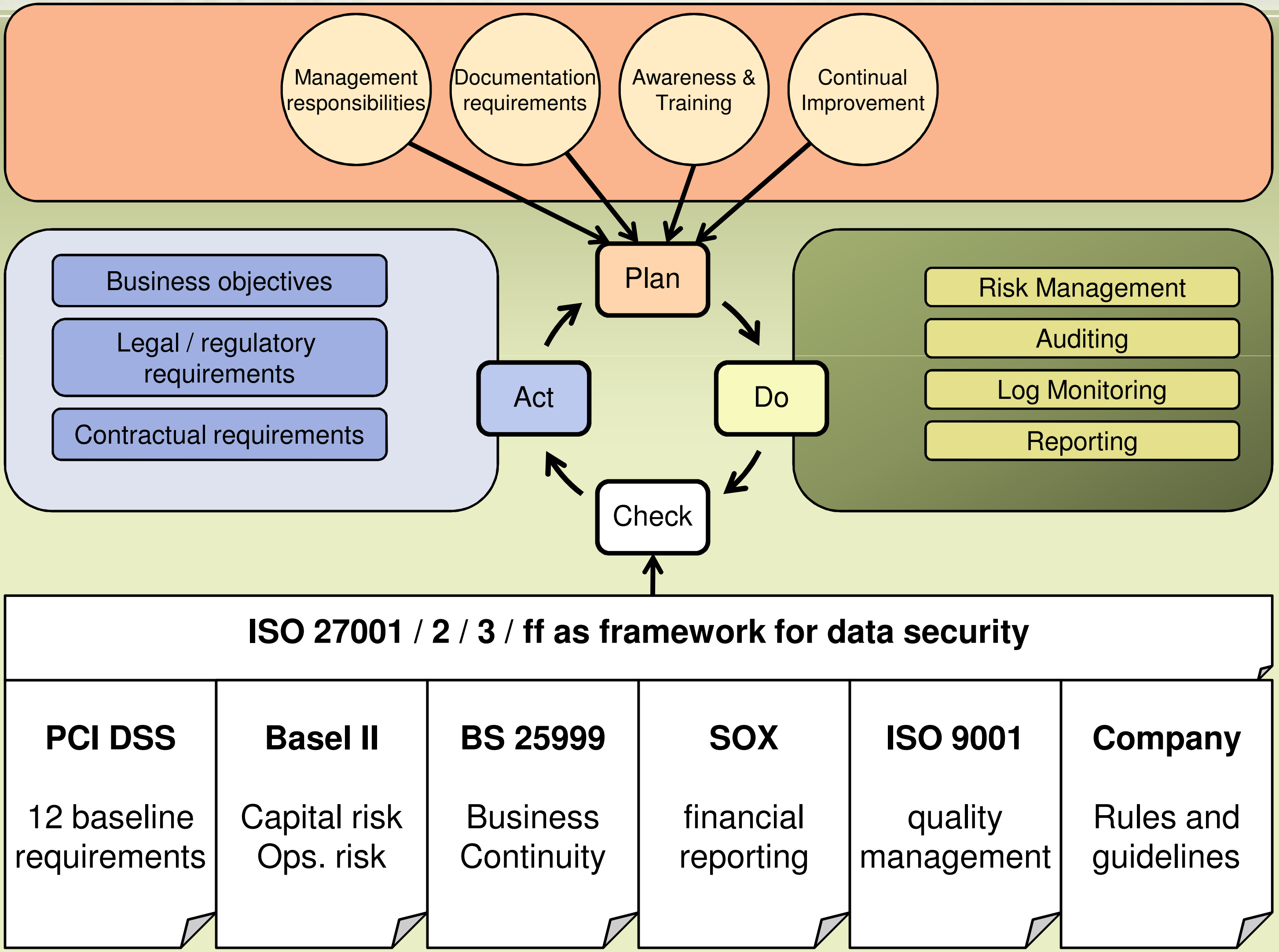
Lessons from the „Heartland“ case

Source : Computerworld

- „The QSA‘s let us down“
- „…had implemented each and every security control of the PCI standard….“
- „industry standard security controls do little to stop lawsuits against you for <u>negligence</u>…“
- Compliance is <u>not</u> taking away any responsibility from you
- When things go wrong, you <u>are</u> (b)eaten by your contracted partners
- Passing a PCI compliance audit does not make you secure
- The QSA factor

- **However :**
- there is <u>no way around PCI</u> – it remains a <u>contractual obligation</u>
- Compliance is not an option
- Opportunity / Risk

ISMS using a unified Compliance framework



The 2 Dimensions of Reducing Risk

Reduce Probability of Incident

- Authentication control
- Access restriction policies
- Password mangement
- Encryption
- Usage restricition of administrative tools
- Time based access control
- Change control procedures
- Software updates
- Vulnerability management
- Policies for reporting weaknesses
- …

Reduce Impact of Incident

- Real time event Monitoring of user activities
- Detection of unauthorized actions
- Filtering, Alerting and Escalation
- Monitoring and reporting of security Events
- Log Management
- File Integrity Monitoring
- Network intrusion detection
- O/S level intrusion detection
- …

CSP Security.com
SOLUTIONS FOR HP NONSTOP SERVERS

CSP Solutions of interest to you !

Reduce Probability of Incidents

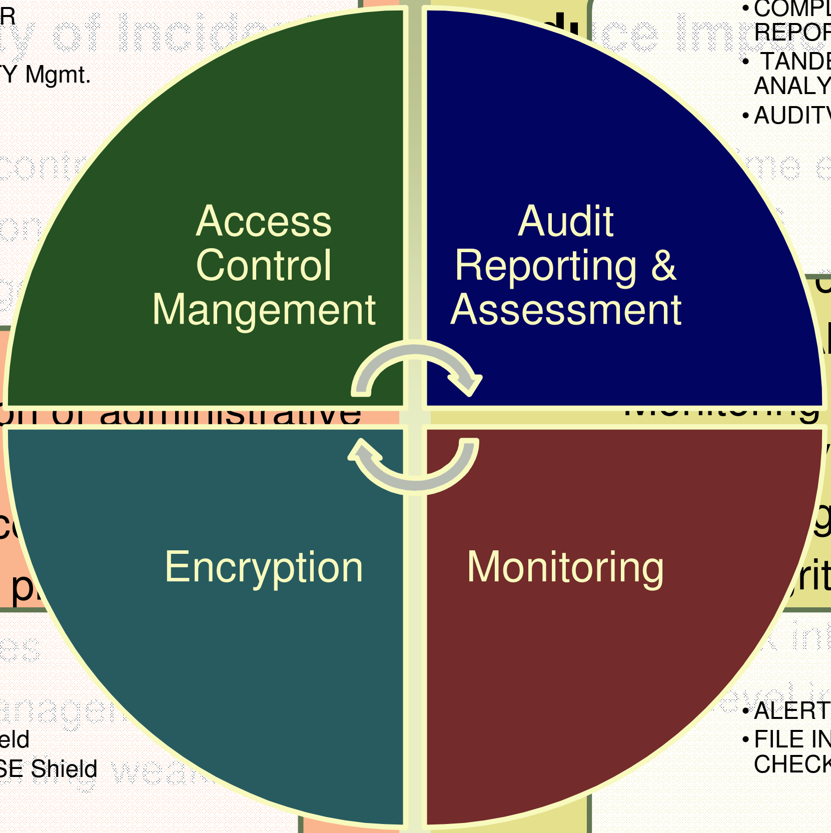
- Authentication control
- Access restriction
- Password mangement
- Encryption
- Usage restricition of administrative tools
- Time based acc
- Change control p
- Software updates
- Vulnera
- Policies reporting wea

duce Impact of Incident

- me event Monitoring of user
- of unauthorized actions
- lerting and Escalation
- and reporting of ents
- gement
- rity Monitoring
- intrusion detection
- evel intrusion detection

- PROTECT XP
- PROTECT UX
- AUTHENTICATOR
- PASSPORT
- Nonstop IDENTITY Mgmt.

- COMPLIANCE REPORTING MODULE
- TANDEM SECURITY ANALYZER
- AUDITVIEW



- FTP Shield
- CLIENT Shield
- ENTERPRISE Shield

- ALERT PLUS
- FILE INTEGRITY CHECKER

Thank you !

**We can‘t solve problems
by using the same kind of thinking
we used, when we created them.**

(Albert Einstein)

For additional information please contact

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