

Protecting other people's money

Who should be PCI DSS compliant and how?

Bob Tarzey,
Service Director
Quocirca Ltd



April 22nd 2010

1. Opportunity

- Compliance is becoming mandatory –varies by brand and region

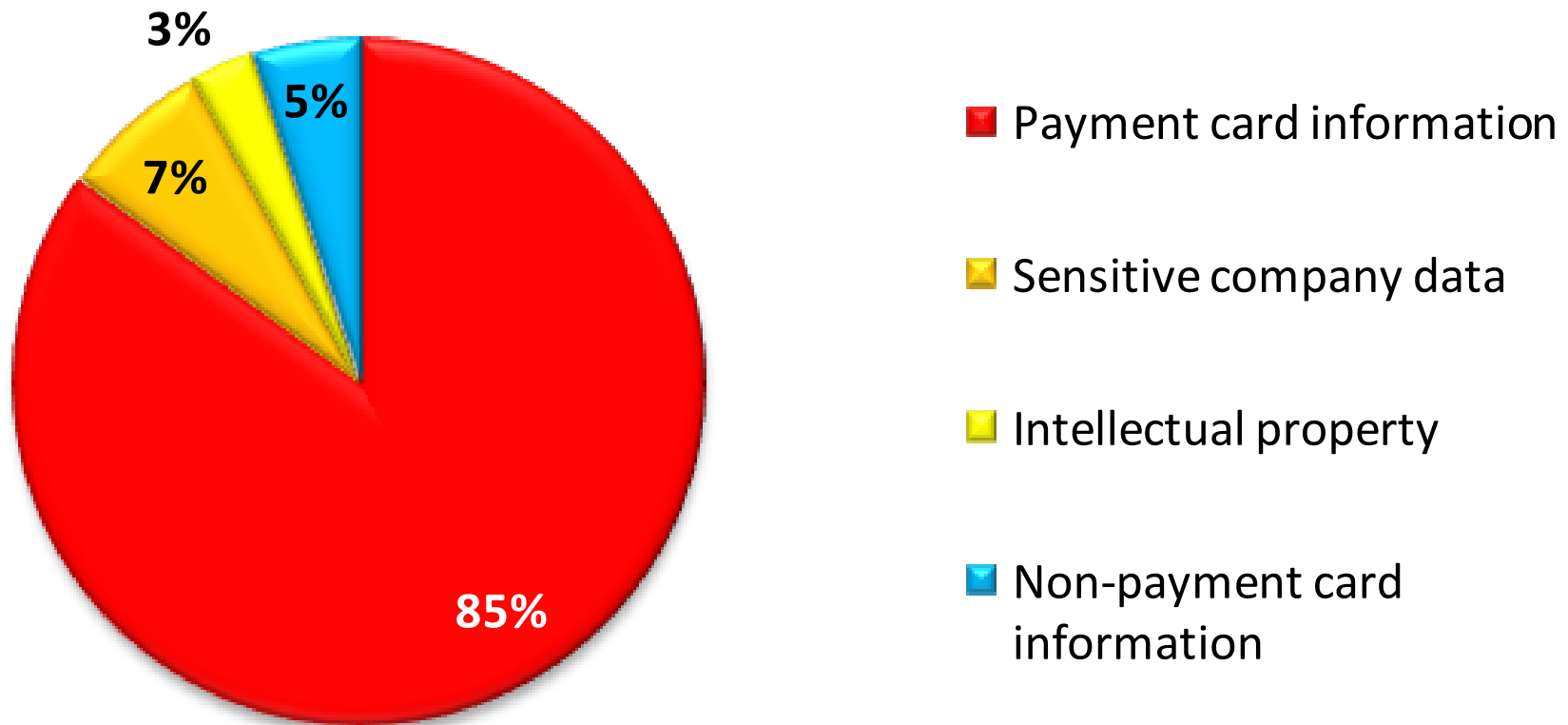
2. Services

- General audit and advice
- PCI relates services (QSA – Qualified Security Assessor)
- Overall compliance

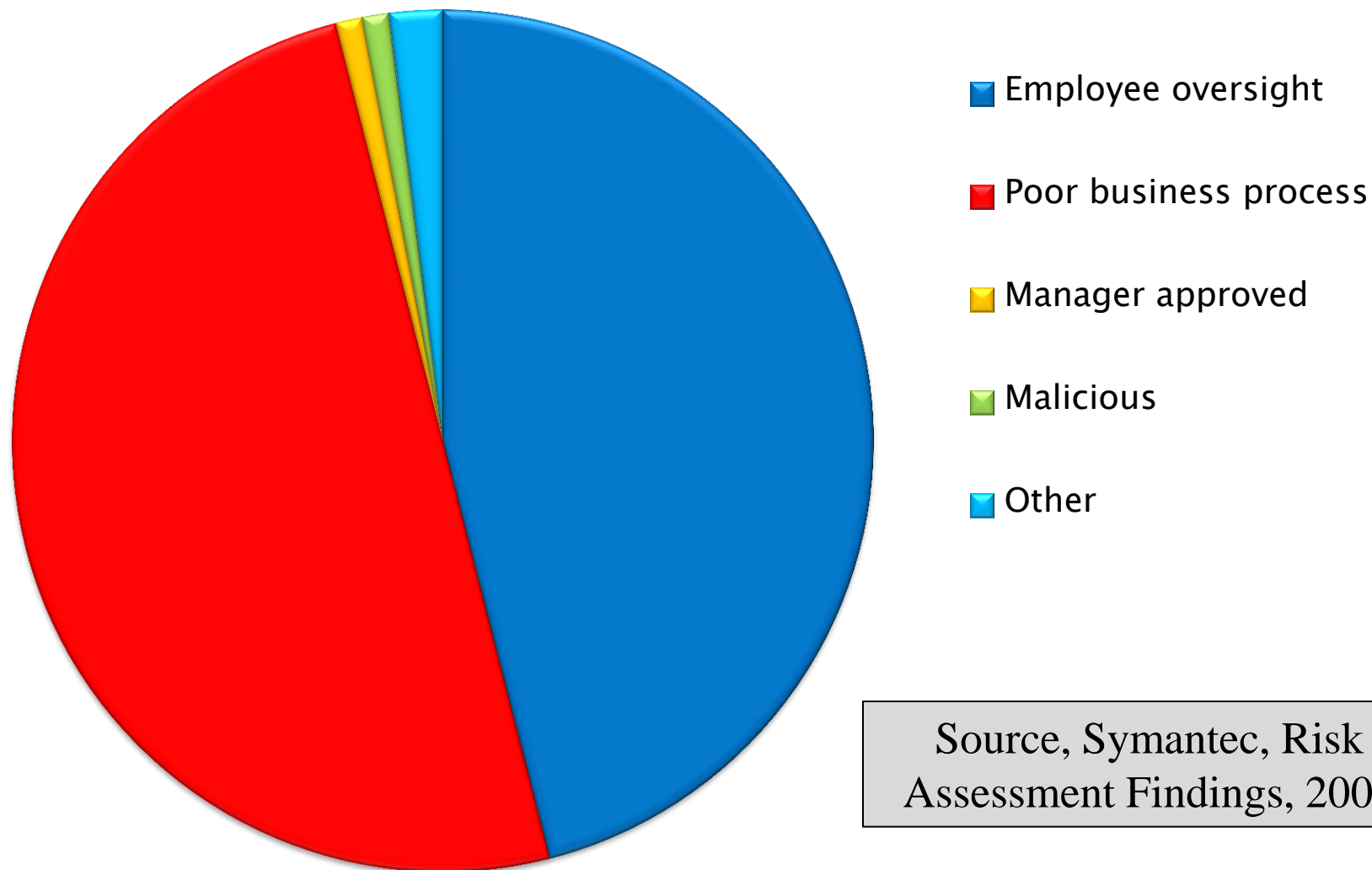
3. Product sales

- Plugging the gaps

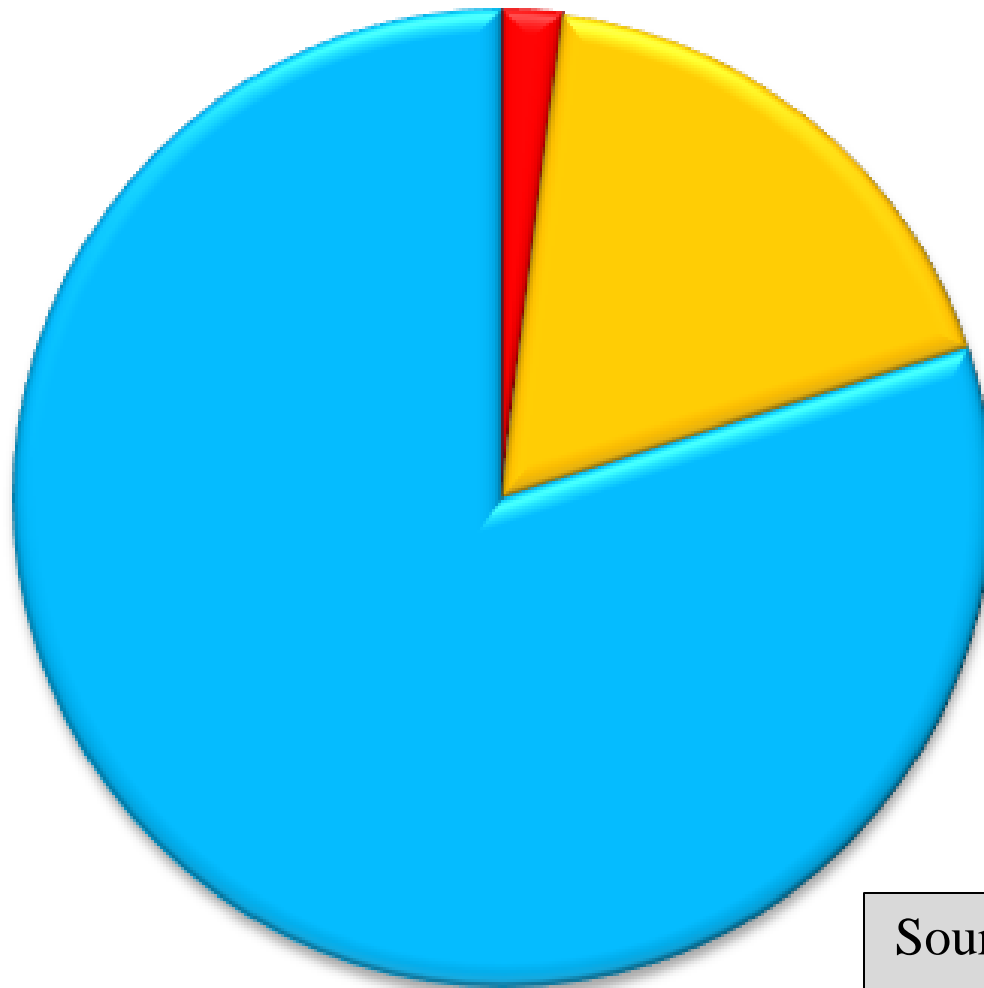
Data types involved in cases of compromised data - from 7Safe UK Security Breach Report (2010)



Causes of leaks – mostly internal



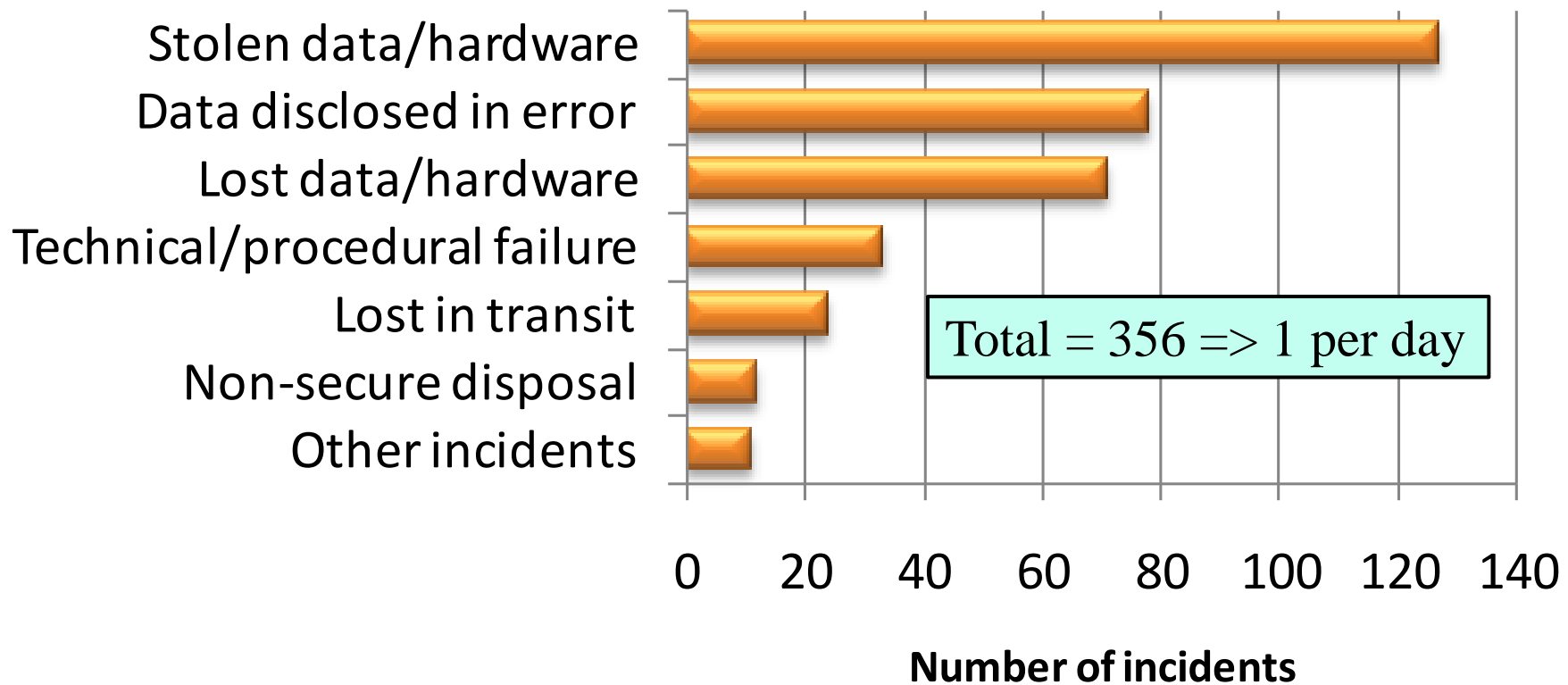
Source, Symantec, Risk Assessment Findings, 2009



- Internal
- Business partner
- External

Source, 7 Safe, UK Security Breach Investigations Report, 2010

Self-reported data breaches - Nov 08 to Aug 09 - UK FOI request



- **Actions following compromise (VISA)**
 - Contact law enforcement
 - Contact bank
 - Contact VISA fraud control
 - Preserve logs
 - Make note of all these actions

VISA “Make sure you have a written policy with an incident response plan and make sure all employees are aware of it”

PCI spokesperson

“It is not enough to be compliant; you need to be secure”

Potential costs

- Fines levied for non-compliance
- Fines levied for breaches
- Fines from other regulators?
- Stolen money

USA 2008: Heartland Payment Systems ordered to pay \$60M to Visa and \$3.6M to Amex for losses they incurred due to the breach of 130 million credit card user records (hackers)

UK March 2010: Argos, exposed as having included credit card detail in HTML code in emails confirmation to customers, said to include CCV data – outcome TBD

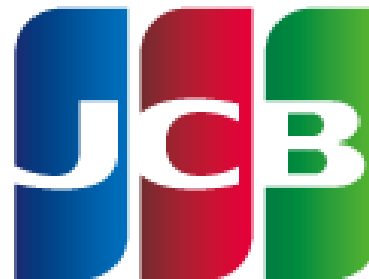
USA 2006 onwards: theft from the retailer TJX of millions sets of credit card details over an 18 month period – \$10m fine (Hacker Albert Gonzalez just got 20 years – 2010)

UK 2007: Nationwide Building Society – fined ~£1M for the loss of PC with unencrypted customer data – size of fine due to poor underlying policy and practice exposed

Payment Cards Industry
Security Standard Council



5 members:



“Both PCI DSS and the payment card brands strongly discourage storage of cardholder data by merchants and processors.

There is no need, nor is it allowed, to store the full magnetic stripe on the back of a payment card.

If merchants or processors have a business reason to store front-card information, such as name and account number, PCI DSS requires this data to be encrypted or made otherwise unreadable.”

PCI SSC web site

What can you store?

Just 4 items – nothing else



Plus: “service code”

- **Secure network**
 1. Firewall
 2. No default passwords
- **Protect data**
 3. Protect stored data
 4. Encrypt transmitted data
- **Vulnerability protection**
 5. Anti-virus
 6. Secure applications
- **Strong access control**
 7. Need to know
 8. Unique Ids
 9. Physical access
- **Monitor and test networks**
 10. Audit access
 11. Test security regularly
- **Have a security policy**
 12. Both for internal and external users

234 sub-requirements

- Merchants
 - Level 1 - > 6M TPY (& “global merchants”)
 - Level 2 - 1M to 6M TYP
 - Level 3 - 20K to 1M TYP
 - Level 4 - < 20K TPY
- Service providers/acquirers
 - Level 1 - > 300K trans/year
 - Level 2 - < 300K trans/year

Taken from:



“PCI compliance is required for any business that accepts payment cards – even if the quantity of transactions is just one” – PCI SSC web site

- The compliance details vary by PC provider
 - All compliance dates for VISA merchants have passed
- You can outsource to compliant service providers, but:
 - Still need to make sure internal processes are compliant
- PCI DSS applies even if using chip and pin machines

QSA – Qualified Security Assessors

ASV – Approved Scanning Vendor

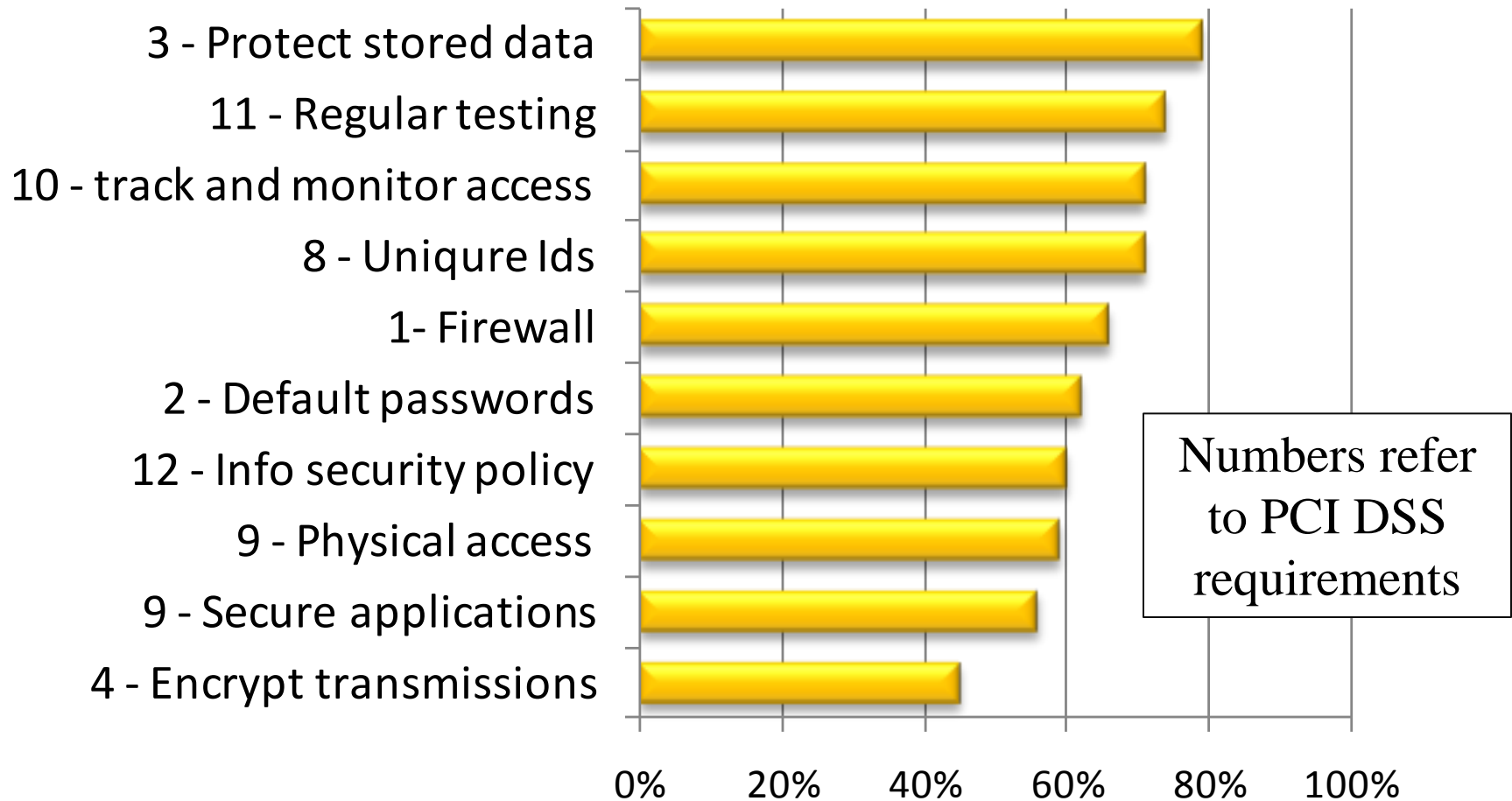
SAQ – Self-Assessment Questionnaire

What level of assessment is necessary?

- Level 1
 - Annual report by QSA
 - Quarterly scan by ASV
 - Attestation of Compliance Form
- Level 2
 - Annual SAQ
 - Quarterly scan by ASV
 - Attestation of Compliance Form
- Level 3
 - Annual SAQ
 - Quarterly scan by ASV
 - Attestation of Compliance Form
- Level 4
 - Annual SAQ recommended
 - Quarterly network scan by ASV if applicable
 - Compliance validation requirements set by acquirers

Taken from: 

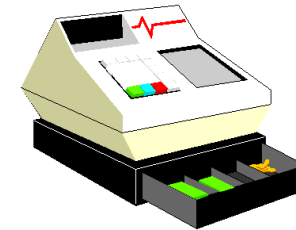
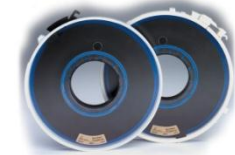
Note: Brand signs off compliance not QSA



VeriSign – Lessons learned: top reasons for PCI audit failure and how to avoid them (2007)

Examples of reasons for audit failure

- Unsecured physical assets
- PoS application vulnerabilities
- Unencrypted spreadsheets
- Poor ID management
- Network design issues
- Lack of log monitoring and IDS



VeriSign – Lessons learned: top reasons for PCI audit failure and how to avoid them (2007)

PCI DSS accepts that not all security measures can be achieved at once:

1. Remove sensitive authentication data and limit retention
2. Protect the perimeter, internal and wireless networks
3. Secure PC applications
4. Monitor and control access to systems
5. Protect stored cardholder data
6. Finalise milestone requirements

All is negotiable as long as progress is being made towards compliance

From PCI SSC “The Prioritized Approach to Pursue PCI DSS Compliance”

- PCI DSS compliance is a moving target (next update Oct 2010)
- No single security vendor can make you compliant
- Advisors are the key; resellers, consultants (QSA)
- PCI makes sense; the standard is good for most sensitive data handling requirements as part of achieving a *compliance oriented architecture*

Thanks, this presentation will be available on
www.quocirca.com

Thank you
Bob Tarzey
Quocirca
[**www.quocirca.com**](http://www.quocirca.com)