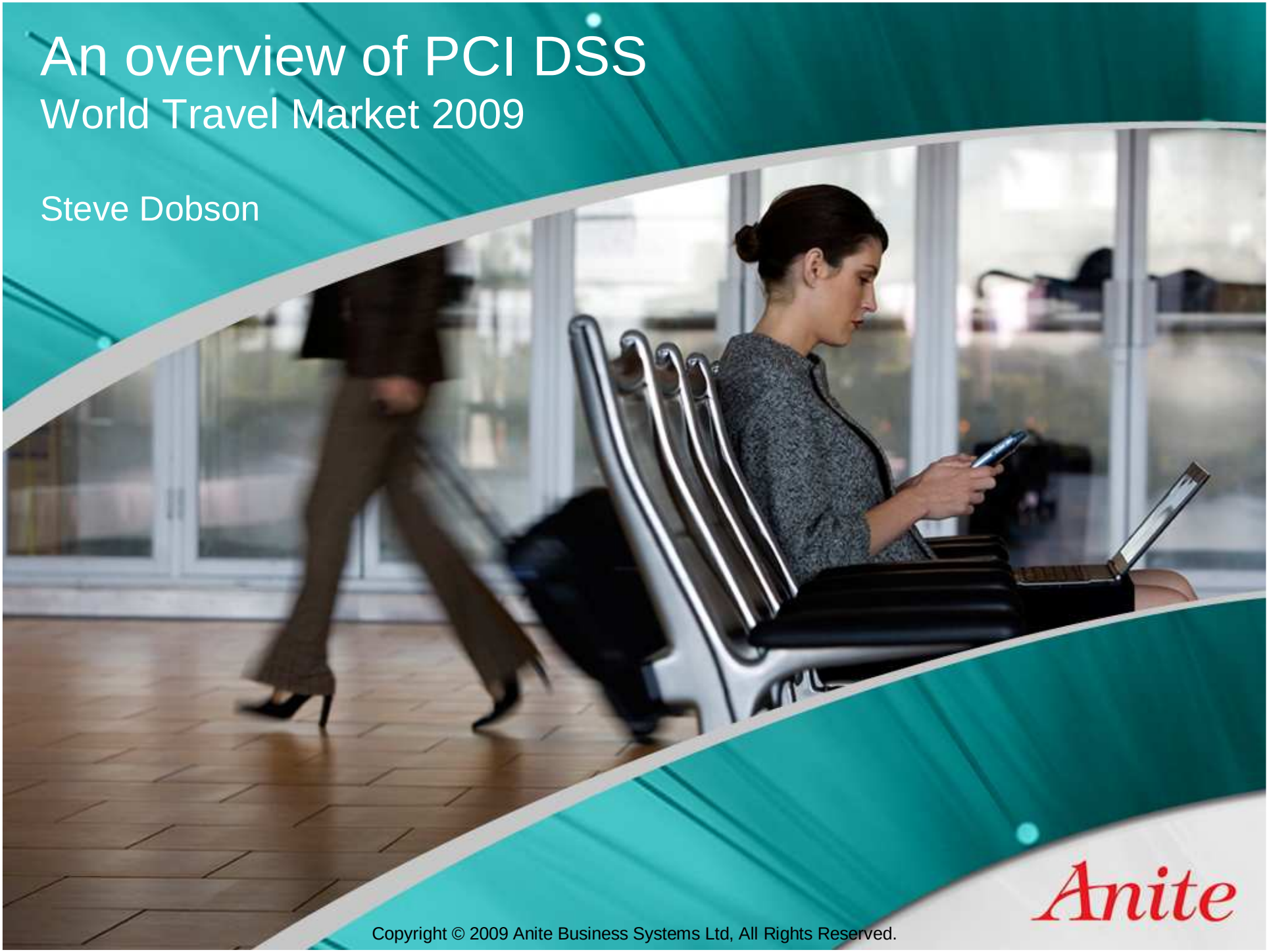
An overview of PCI DSS

World Travel Market 2009

Steve Dobson



Anite

What is PCI DSS and who does it apply to ?

- PCI = Payment Card Industry
  - Global body founded by:

- DSS = Data Security Standard
  - ***Aims*** to ensure card data is protected from theft and unauthorised use
- Who ?
  - Merchants or organisations that store, process or transmit cardholder data
  - Compliance is compulsory
    - Non compliance means no card processing contract

Anite

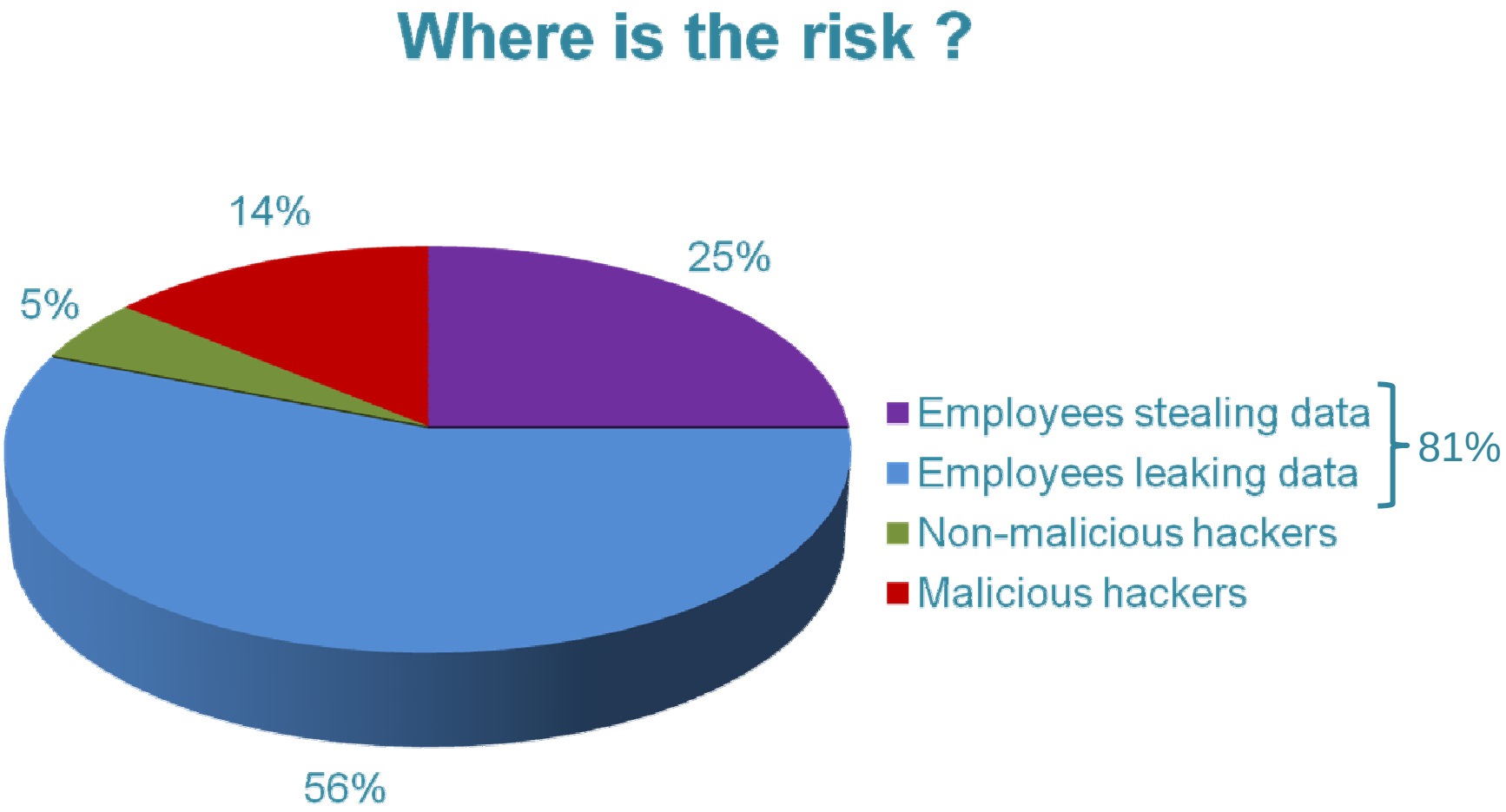
Why do we need to do this, it will never happen to us !

That's what these companies thought:

- 2009 - Heartland Payment Systems – 100M cards
- 2008 – RBS Worldpay – 1.5M cards
- 2008 - Hannaford Brothers Co. – 4.2M cards
- 2007 – TJX Companies Inc – 45M cards
- 2005 - CardSystems Solutions 40M cards

The potential fine for each card number stolen is $25 !

A Security Statistic



Source: Secure Computing

The goals and requirements of the standard

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for employees and contractors

Anite

How do we get certified ?

- Get a PCI certified auditor
  - Qualified Security Assessor, PCI-QSA
- Perform a gap analysis with this auditor
  - this could save you a lot of cost and effort in the longer term
- Determine which compliance document you need to complete (Self Assessment Questionnaire)
  - SAQ-A for companies who outsource their systems to a certified systems provider
  - SAQ-D for everyone else
- Plan and Implement

Anite

How long will it take ?

- SAQ-A
  - New policies and procedures
  - Security awareness training
  - 2 to 3 weeks

- SAQ-D
  - New policies and procedures
  - Security awareness training
  - Network revamp
  - Application software modifications
  - System hardening
  - 3 to 6 months (if you are lucky)

Estimates assume that this is a Tour Operator taking bookings over the phone and through the Internet

Anite

Resources

Web site

- https://www.pcisecuritystandards.org

The definitive resource for everything to do with PCI security standards

- PCI Quick Reference Guide

A useful guide that provides a good overview of the PCI DSS standard

- PCI DSS v1.2

The standard (73 pages)