



Securing Card Payments

CQR Consulting



- ▶ Global, Independent, Information Security Specialists
- ▶ Adelaide Head Office
- ▶ Qualified Security Assessors
- ▶ Assist organisations to identify and manage their business risks



Some Terminology

- ▶ PCI DSS - Payment Card Industry Data Security Standard
- ▶ QSA - Qualified Security Assessor
- ▶ ASV - Approved Scanning Vendor
- ▶ Merchant - An entity that accepts credit cards
- ▶ Acquirer - Card association member that interacts with merchants to settle transactions

Quick History Lesson

- ▶ PCI Security Standards Council
 - American Express, Discover, JCB, MasterCard, Visa
- ▶ PCI SSC wrote the DSS
- ▶ Since December 2004
- ▶ Currently Version 1.1
 - Version 1.2 due 1st October 08

12 Requirements

- ▶ Secure Network
 - Firewall and passwords
- ▶ Protect Card Data
 - Protect stored data and encrypt transmission
- ▶ Vulnerability Management Program
 - Antivirus Software
 - Secure Systems and applications
- ▶ Strong Access Control Measures
 - Restrict Access – electronic and physical
 - Unique ID's
- ▶ Monitor and Test
 - Track and monitor access to card data and test
- ▶ Information Security Policy
 - Maintain a policy that addresses Information Security



Easy Wins

- ▶ Don't store credit card numbers
- ▶ Network Segregation
 - Limit the size of the area where the card numbers are kept
- ▶ Compensating Controls
 - Protection
- ▶ Limit and log the access
 - Essential access to card numbers

Recent Incidents

- ▶ TJX – 45.7 Million cards
- ▶ Hannaford Bros – 4.2 Million cards
- ▶ Best Western Hotels 8 Million cards (allegedly)
- ▶ Roses Only
- ▶ CQR Consulting Engagements
 - Accessed cards via internet
 - Storing card details in clear text

Consequences

- ▶ Penalties - Financial
 - Fines
 - Higher Transaction Rates
- ▶ Prevention from accepting credit cards (either enforcement or choice)
- ▶ Legal
- ▶ Regulatory Bodies

What can you do?

- ▶ Engage with your acquirer
- ▶ Speak to a QSA
 - We're not the 'PCI DSS Police'
- ▶ Speak to vendors
- ▶ Make sure that PCI compliance is a component of tenders or contracts
- ▶ Don't bury your head in the sand - this isn't going away



Questions?



- ▶ CQR Consulting
- ▶ pci@cqrconsulting.com
- ▶ 08 8364 5881
- ▶ www.pcisecuritystandards.org

