



build | integrate | secure

Grow with Denim Group



PCI Compliance for Your Organization  
John B. Dickson, CISSP  
October 11, 2007

# Learning objectives for today's session

- Overview of PCI – who, what, why...
- Overview of PCI Data Security Standard
- Understand which organizations are affected by PCI
- Understand approaches to comply with PCI

# Denim Group Background

- Professional services firm that builds and secures enterprise web applications
- Application security services include:
  - *Black-box and white-box assessments*
  - *Secure application development and remediation*
  - *Application security training for developers, security professionals, and auditors*
  - *Software development lifecycle development (SDLC) consulting*
  - *Application identity management enablement*
- Competencies in the following areas:
  - *PCI Pre-assessment readiness*
  - *Secure agile development*
  - *Threat modeling*

# Personal Background

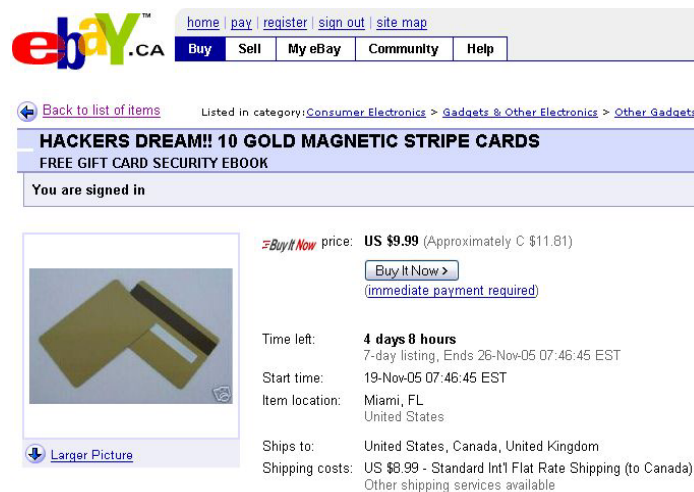
- 15-year information security consultant background
- Principal at Denim Group
- Ex-Air Force, Trident Data Systems, KPMG, and SecureLogix information security consultant
- Strong system and application development background
- CISSP since 1998
- Worked on several PCI pre-assessment readiness efforts

# What is PCI?

- Payment Card Industry Security Standards Council (PCI)
  - *Worldwide credit card consortium organized to provide develop, publish, and continually improve data security standards for card accounts*
  - *Founded 2006 by Visa, MasterCard, AMEX, Discover, and JCB*
  - *Publishes and updates the PCI Data Security Standard (DSS)*
  - *Certifies and set standards for assessor and scanning vendors*
  - *Over 150 organizations involved worldwide*

# Why PCI?

- Risk losing the ability to process credit card transactions
- Organizations can incur fines for non compliance
- General embarrassment



The screenshot shows an eBay listing for "HACKERS DREAM!! 10 GOLD MAGNETIC STRIPE CARDS". The listing includes a "Buy It Now" price of US \$9.99, a "Time left" of 4 days 8 hours, and a "Shipping costs" of US \$8.99. The listing is for 10 gold magnetic stripe cards, with a free gift card security ebook included. The listing is located in Miami, FL, and ships to the United States, Canada, and the United Kingdom.


home | pay | register | sign out | site map

Buy Sell My eBay Community Help

Back to list of items Listed in category: Consumer Electronics > Gadgets & Other Electronics > Other Gadgets

**HACKERS DREAM!! 10 GOLD MAGNETIC STRIPE CARDS**  
FREE GIFT CARD SECURITY EBOOK

You are signed in

 **Buy It Now** price: **US \$9.99** (Approximately C \$11.81)

[Buy It Now >](#)  
(immediate payment required)

Time left: **4 days 8 hours**  
7-day listing, Ends 26-Nov-05 07:46:45 EST

Start time: 19-Nov-05 07:46:45 EST

Item location: Miami, FL  
United States

Ships to: United States, Canada, United Kingdom

Shipping costs: US \$8.99 - Standard Int'l Flat Rate Shipping (to Canada)  
Other shipping services available

[Larger Picture](#)

# Key PCI Definitions

- *PAN – Primary Account Number - the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. Also called Account Number*
- *QSA – Qualified Security Assessor – organizations that validate an entity's compliance with PCI DSS requirements*
- *ASV - Approved Scanning Vendor – organizations that validate adherence to PCI DSS requirements by conducting vulnerability scans of Internet-facing environments of merchants and service providers*
- *Service Providers - Business entity that is not a payment card brand member or a merchant directly involved in the processing, storage, transmission, and switching or transaction data and cardholder information or both. This also includes companies that provide services to merchants, services providers or members that control or could impact the security of cardholder data.*

# Who's covered by PCI?

- The Payment Card Industry Data Security Standard (PCI DSS) applies to every organization that processes credit or debit card information, including merchants and third-party service providers that store, process or transmit credit card/debit card data.
  - *Originally, if you store, process or transmit the Primary Account Number (PAN)*

# Compliance Levels

- Level 1:
  - *Merchants with more than 6,000,000 transactions per year. Other merchants in Level 1 will be merchants whose security has been violated and data compromised and merchants which another credit card company have classified as Level 1*
- Level 2:
  - *Merchants with 150,000 to 6,000,000 transactions per year.*
- Level 3:
  - *Merchants with 20,000 to 150,000 transactions per year*
- Level 4
  - *Merchants with less than 20,000 transactions per year*

# Data Security Standard (DSS)

- Version 1.1, Published September 2006
- Grouped into 12 control objectives by the following:
  - *Build and Maintain a Secure Network*
  - *Protect Cardholder Data*
  - *Maintain a Vulnerability Program*
  - *Implement Strong Access Control Measures*
  - *Regularly Monitor and Test Networks*
  - *Maintain and Information Security Policy*

Source: PCI DSS 1.1

# Data Security Standard (DSS)

- Build and Maintain a Secure Network
  - *Requirement 1: Install and maintain a firewall configuration to protect cardholder data*
  - *Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters*

Source: PCI DSS 1.1

# Data Security Standard (DSS)

- Protect Cardholder Data
  - *Requirement 3: Protect stored cardholder data*
  - *Requirement 4: Encrypt transmission of cardholder data across open, public networks*

Source: PCI DSS 1.1

# Data Security Standard (DSS)

- Maintain a Vulnerability Management Program
  - *Requirement 5: Use and regularly update anti-virus software*
  - *Requirement 6: Develop and maintain secure systems and applications*

Source: PCI DSS 1.1

# Data Security Standard (DSS)

- Implement Strong Access Controls
  - *Requirement 7: Restrict access to cardholder data by business need-to-know*
  - *Requirement 8: Assign a unique ID to each person with computer access*
  - *Requirement 9: Restrict physical access to cardholder data*

Source: PCI DSS 1.1

# Data Security Standard (DSS)

- Regularly Monitor and Test Networks
  - *Requirement 10: Track and monitor all access to network resources*
  - *Requirement 11: Regularly test security systems and processes*

Source: PCI DSS 1.1

# Data Security Standard (DSS)

- Maintain an Information Security Policy
  - *Requirement 12: Maintain a policy that addresses information security*

Source: PCI DSS 1.1

# Data Security Standard (DSS)

- Implement Strong Access Controls
  - *Requirement 7: Restrict access to cardholder data by business need-to-know*
  - *Requirement 8: Assign a unique ID to each person with computer access*
  - *Requirement 9: Restrict physical access to cardholder data*

Source: PCI DSS 1.1

# Conclusions

- PCI is an absolute must for those that process credit card numbers
- PCI compliance can be complex and expensive for large volume processors with distributed credit card systems
- PCI DSS is driving certain technical compliance activities that did not exist prior
- Security managers can learn from PCI DSS, regardless of whether organizations have to comply

# References

- *PCI Security Standards Council* - <https://www.pcisecuritystandards.org/>
- *Forrester Group*, “The Top 10 Things You Should Know About PCI Compliance,” [Khalid Kark](#), [Chris McClean](#) with [Jonathan Penn](#)
- *Gartner Group*, “The Payment Card Industry Must Disentangle PCI Assessments From Remediation,” [John Pescatore](#)

# Questions & Answers

***John B. Dickson, CISSP***

*(210) 572-4400*

*john@denimgroup.com*