

camex

Campus Market Expo 2008

Igniting Collegiate Retailing



National Association
of College Stores

CONNECT | GROW | SUCCEED

Data Security Practices

Kevin Wright

Vice President of Information Technology
Nebraska Book Company

Session #6-01 Saturday, March 1, 2008



Presentation Format

- Introduction
- Best Practices
- Payment Card Industry (PCI DSS)
- Summary
- Question & Answer



Introduction

- My Background / Perspective
 - Over 25 years IT experience
 - Nebraska Book
 - Over 250 retail stores
 - Over 1000 stores using NBC software
 - Over 800 stores using NBC as ASP
- Disclaimer !!!



Data Security

- History
- Types
- Importance
- Risks



Security Breaches

- Fidelity National – 8.5 million
 - Britain's Tax & Customs - 25 million
 - Dai Nippon Printing – 43 million
 - TD Ameritrade – 6.3 million
 - Monster – 1.3 million
 - TJX – 46 million
 - Card Systems – 40 million
 - **EXPENSIVE !!!!**
- 

Best Practices - Overview

- Take Stock – Know what you have.
- Scale Down – Keep just what you need
- Lock It – Protect what you keep.
- Pitch It – Dispose of what you don't need.
- Plan Ahead – Have an incident plan.




Best Practices – Take Stock

- Inventory your files and computers to see what information you have.
- Where is it collected, where is it held, how is it used, how long is it needed?
- Also take stock of industry regulations or laws that may impact your business.
- Rate the risk.



Best Practices – Scale Down

- Keep only what you NEED for your business.
 - Don't use SSN's or other sensitive data as account numbers.
 - Don't keep sensitive data longer than necessary.
 - Minimize the number of people that have access to sensitive data.
 - Minimize the number of places sensitive data is kept.
- 

Best Practices – Lock It

- Physical Security
 - Locks, Limit & Control Access
- Electronic Security
 - Firewalls, IDS, AntiVirus, Patches, Encryption
- Employee Training
 - Document policies, background checks, culture of security
- Service Providers / Contractors



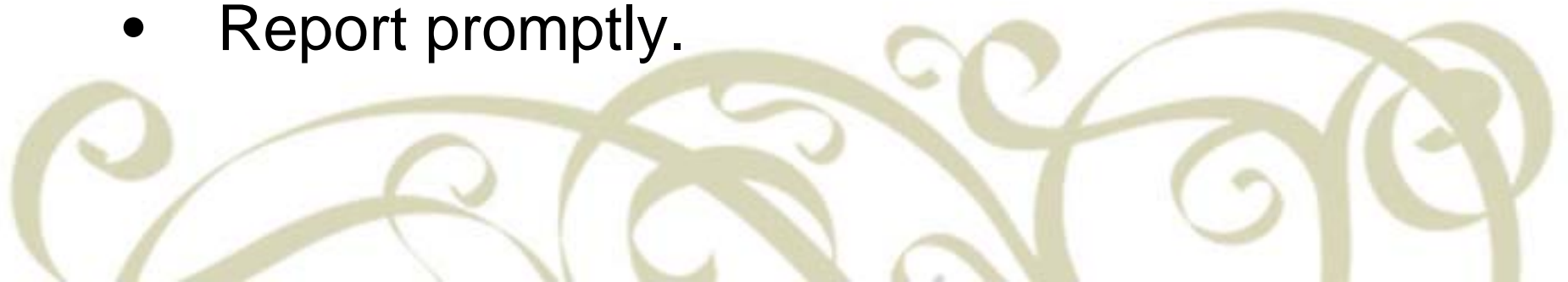
Best Practices – Pitch It

- Implement reasonable disposal practices.
- Dispose of physical copies by shredding.
- Use specialized “wipe” programs to remove electronic copies.
- Ensure employees working from home or on other systems follow same procedures.
- If you use background checks, you may be subject to the FTC’s Disposal Rule.



Best Practices – Plan Ahead

- Have a plan in place to respond to security incidents.
- Designate a senior staff member to coordinate and implement plan.
- If a computer is compromised, disconnect it from the network.
- Investigate immediately.
- Report promptly.



Best Practices - Resources

National Institute of Standards and Technology Computer Resource Center

www.csrc.nist.gov

SANS Institute Twenty Most Critical Internet Security Vulnerabilities

www.sans.org/top20

United States Computer Emergency Readiness Team (US-CERT)

www.us-cert.gov

Open Web Application Security Project

www.owasp.org

Federal Trade Commission's Guide for Information Security

www.ftc.gov/infosecurity



PCI DSS - Introduction

- Payment Card Industry Data Security Standard
- Survey
 - PCI DSS
 - PABP
- History
 - VISA CISP / MC SDP
 - Card Associations / Merchant Banks / Merchants



PCI – What Is It?

- Data Security Standard cover six topic areas and twelve high level requirements.
- Merchants divided into four levels.
- Standard (requirements) same for all levels – auditing and deadlines vary.
- Perform Quarterly Network Scans



PCI – Merchant Levels

Level	Annual Visa/MC Transactions	Validation	Deadline	In Compliance with PCI
Level 1	More than 6 million	Annual Audit Quarterly Scan	9/30/04	77%
Level 2	1 to 6 million	Self Assessment Quarterly Scan	9/30/07	62%
Level 3	20,000 to 1 million	Self Assessment Quarterly Scan	6/30/05	54%
Level 4	Less than 20,000	Self Assessment Quarterly Scan	Merchant Bank Determines	N/A



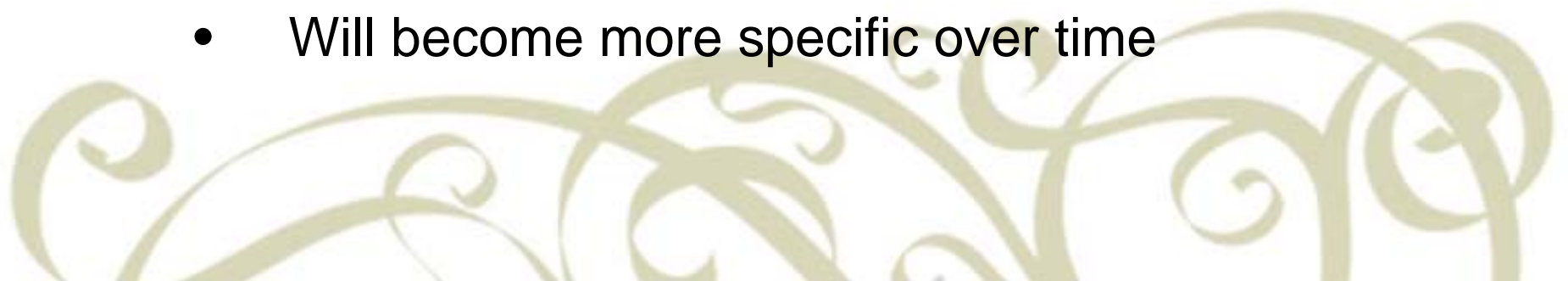
PCI – Requirements

- Build & Maintain a Secure Network
- Protect Cardholder Data
- Maintain Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor & Test Networks
- Maintain an Information Security Policy




PCI – More Details

- Six broad categories translate into over 120 specific requirements.
- PCI is for the Retailer
- No magic bullet
- Evolving Standard – Currently version 1.1
 - Payment Application Best Practices
 - Will become more specific over time



PCI – Recommendations

- Select a knowledgeable partner to work through compliance effort.
 - Use validated payment applications (VISA publishes list)
 - Use best practices – especially Scale Down
 - Rate level of compliance. (Everything isn't black or white.)
 - Show Progress !!!
- 

PCI - Resources

PCI Security Standard Council (Standard, QSA's, self assessment)

<https://www.pcisecuritystandards.org/>

VISA's List of Validated Payment Applications

http://usa.visa.com/download/merchants/validated_payment_applications.pdf

VISA's List of Certified Service Providers

http://usa.visa.com/download/merchants/cisp_list_of_cisp_compliant_service_providers.pdf



Summary

Best Practices

- Take Stock
- Scale Down
- Lock It
- Pitch It
- Plan Ahead

PCI

- Use Best Practices
- Work with Partner
- Use Validated Payment Application
- Show Progress



Question & Answer



Contact Slide

Kevin Wright

Vice President of IT

Nebraska Book Company

Phone: (402) 421-0738

E-mail: kwright@nebook.com

Web: www.nebook.com

