



The Seven Deadly Sins of PCI Compliance



Presenters



- Jerry Trieber, CFE, CFF, CPA, CHAE
Director of Field Accounting, Crestline Hotels & Resorts, Inc.
- Responsible for financial oversight of a portfolio of ten full-service hotels across the United States
- Involved in Crestline's PCI Compliance initiatives
- Involved in Crestline's Sarbanes-Oxley compliance initiatives



- Bill Randall
Director of IT Infrastructure, Red Robin Gourmet Burgers, Inc.
- Responsible for the Infrastructure, Security and Compliance for over 300 Red Robin restaurant locations
- Responsible for Red Robin's PCI compliance initiatives and annual PCI assessment
- Responsible for Red Robin's Sarbanes-Oxley compliance initiatives



Session Objectives

- ❑ Discuss and define the seven deadly sins of PCI Compliance.
- ❑ Discuss the consequences of each “sin.”
- ❑ Discuss proactive techniques to become aware of each “sin.”
- ❑ Discuss combative techniques to diminish the potential impact of each “sin.”
- ❑ Ask questions.
- ❑ Have fun!



The Seven Deadly Sins of PCI Compliance

- ▣ The First Deadly Sin: Sin of Insecurity
- ▣ The Second Deadly Sin: Sin of Ignorance
- ▣ The Third Deadly Sin: Sin of Apathy
- ▣ The Fourth Deadly Sin: Sin of Laziness
- ▣ The Fifth Deadly Sin: Sin of Gluttony
- ▣ The Sixth Deadly Sin: Sin of Over-confidence
- ▣ The Seventh Deadly Sin: Sin of Accessibility



The First Deadly Sin: Sin of Insecurity

- ▣ Generally addressed by PCI DSS Requirement # 9:
“Any physical access to data or systems that house cardholder data ... should be appropriately restricted.”
- ▣ Specifically addressed by PCI DSS Requirement # 9.6:
“Physically secure all paper and electronic media (including computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain cardholder data.”



The First Deadly Sin: Sin of Insecurity

Things to Consider: Electronic Access

Property Management System (PMS)/
Point Of Sale (POS) Access to View
Complete Guest Credit Card Data

- ▣ Review who has access to view a guest's 15 or 16-digit credit card number
- ▣ Access should be adequately restricted (managers, supervisors)



The First Deadly Sin: Sin of Insecurity

Things to Consider: Physical Capture

Physical Imprinting of Credit Cards

- ▣ Review why cards may be imprinted
- ▣ Review proper merchant bank retrieval request and chargeback information requirements
- ▣ Review proper storage of registration cards
- ▣ Imprinting of cards should be extremely limited if at all



The First Deadly Sin: Sin of Insecurity

Things to Consider: Credit Card Pre-Authorization for Sales, Catering, and Banquets

Physical Credit Card Data in Sales files, Catering Files, on Banquet Event Orders (BEOs), and Banquet Checks

- ▣ Guests send card data (via e-mail, facsimile, or paper) to guarantee or pre-pay for a catering event
- ▣ Sales, Catering, and Banquet associates place the card data in a paper-based manila folder, type the card data into the Sales & Catering system (Delphi, SalesPro, e.g.), or write the card data on a paper in the file



The First Deadly Sin: Sin of Insecurity

Things to Consider: Credit Card Pre-Authorization for Sales, Catering, and Banquets

Physical Credit Card Data in Sales files, Catering Files, on Banquet Event Orders (BEOs), and Banquet Checks

- ▣ Where are the Sales files stored?
- ▣ Where are the Catering files stored?
- ▣ What happens to the BEOs?
- ▣ What happens to the banquet checks?
- ▣ What happens to the card data written on a “sticky note” placed on an associate’s computer monitor?



The First Deadly Sin: Sin of Insecurity

Things to Consider: Credit Card Pre-Authorization

At the Front Desk

Credit Card Authorization Forms, Binders, and Accordion Files

- ▣ Guests send card data (via e-mail, facsimile, or paper) to the hotel's front office in advance of a guest's stay
- ▣ Front Desk associates place the card data in a three-ring binder, manila folder, accordion file, or hanging file folder located at or near the Front Desk



The First Deadly Sin: Sin of Insecurity

Things to Consider: Credit Card Pre-Authorization

At the Front Desk

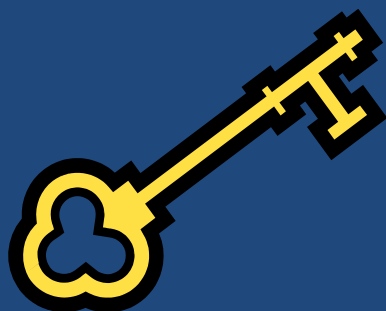
Credit Card Authorization Forms, Binders, and Accordion Files

- ▣ Where are the Credit Card Authorization Forms stored?
- ▣ Where are the Credit Card Authorization Binders stored?
- ▣ Where are the Credit Card Authorization accordion files stored?



The First Deadly Sin: Sin of Insecurity

The



is



!

- ▣ ALL documents containing credit card data MUST be properly secured (under lock and key) with restricted access at all times.
- ▣ Understand the business need and process for retaining cardholder data (Requirement 7).
- ▣ Treat cardholder data like the crown jewels!





The Second Deadly Sin: Sin of Ignorance

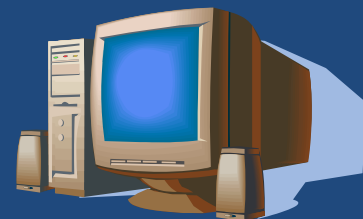
- ▣ Generally addressed by PCI DSS Requirement # 6:
“All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses.”
- ▣ Specifically addressed by PCI DSS Requirement # 6.1:
“Ensure that all system components and software have the latest vendor-supplied...patches installed. Install relevant ...patches within one month of release.”



The Second Deadly Sin: Sin of Ignorance

Things to Consider: Technology Inventory

- ▣ A technology inventory should be taken not less than annually of the following:
 - ▣ Property Management System (PMS) version
 - ▣ Point of Sale System (POS) version
 - ▣ Reservation System (CRS/GDS version)
 - ▣ Middleware version
 - ▣ Merchant Bank
- ▣ All systems above **MUST** be using the most current version!

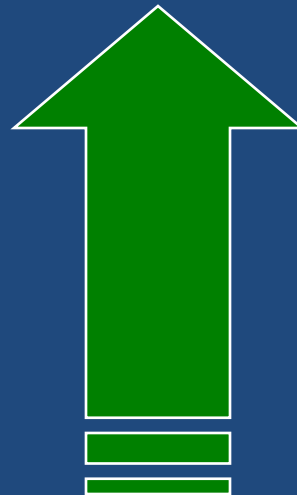




The Second Deadly Sin: Sin of Ignorance

Things to Consider: Technology Upgrades



- ▣ Upgrades based upon technology inventory
- ▣ Contact vendors for pricing and installation
- ▣ Cost may seem expensive but is less costly than potential penalties, negative press, and reputation damage!





The Second Deadly Sin: Sin of Ignorance

Things to Consider: Technology Compliance Sources

- ▣ VISA CISP (Cardholder Info. Security Program) 
http://usa.visa.com/merchants/risk_management/cisp_tools_faq.html
- ▣ MasterCard SDP (Site Data Protection Program) 
<http://www.mastercard.com/us/merchant/security/requirements.html>



The Second Deadly Sin: Sin of Ignorance

Things to Consider: Technology Compliance Sources

- ▣ Discover DISC (Discover Information Security & Compliance)



<http://www.discovernetwork.com/fraudsecurity/disc.html>

- ▣ American Express DSOP (Data Security Operating Policy)



https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=home&ln=en&frm=US



The Third Deadly Sin: Sin of Apathy

- ▣ Generally addressed by PCI DSS Requirement # 12:
“Maintain a policy that addresses information security for employees and contractors.”
- ▣ Specifically addressed by PCI DSS Requirement # 12.10:
“All processors and service providers must maintain and implement policies and procedures to manage connected entities, to include...ensur[ing] the entity is PCI DSS compliant....”



The Third Deadly Sin: Sin of Apathy

Things to Consider: Reliance on Brand/Franchisor Rules, Policies, and Technology

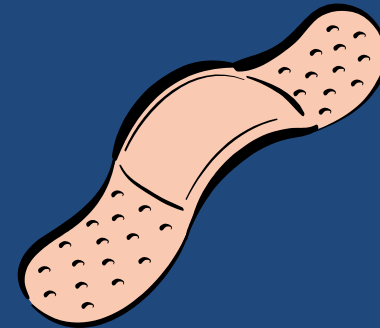
- ▣ Operators must be sure that they are using the most current versions of their franchisor's technologies, including PMS and POS hardware and software.





The Third Deadly Sin: Sin of Apathy

- ▣ Network Testing and Scanning
 - Internal/External Penetration Tests
 - Self scanning
 - ▣ Automate
 - ▣ Review
 - ▣ Remediate
- ▣ Patching and Updates
 - Antivirus/Spyware /Malware
 - OS Patching
 - Application Patching





The Third Deadly Sin: Sin of Apathy

Patching Process



Review

Read up on the impacted change
Determine the fit by server function

Test

Create a script

Validate

Did it fix the documented issue?
Did it “break” any other functionality?

Deploy

Check that it was successfully deployed





The Fourth Deadly Sin: Sin of Laziness

Keeping Default/Common Passwords

- ❑ Review/Document all applications and access
- ❑ Identify applications that...
 - Process, store, or transmit cardholder data
 - Provide access to the cardholder environment
 - Should be physically separated on the network
 - Directly interface with cardholder applications





The Fourth Deadly Sin: Sin of Laziness

Keeping Default/Common Passwords

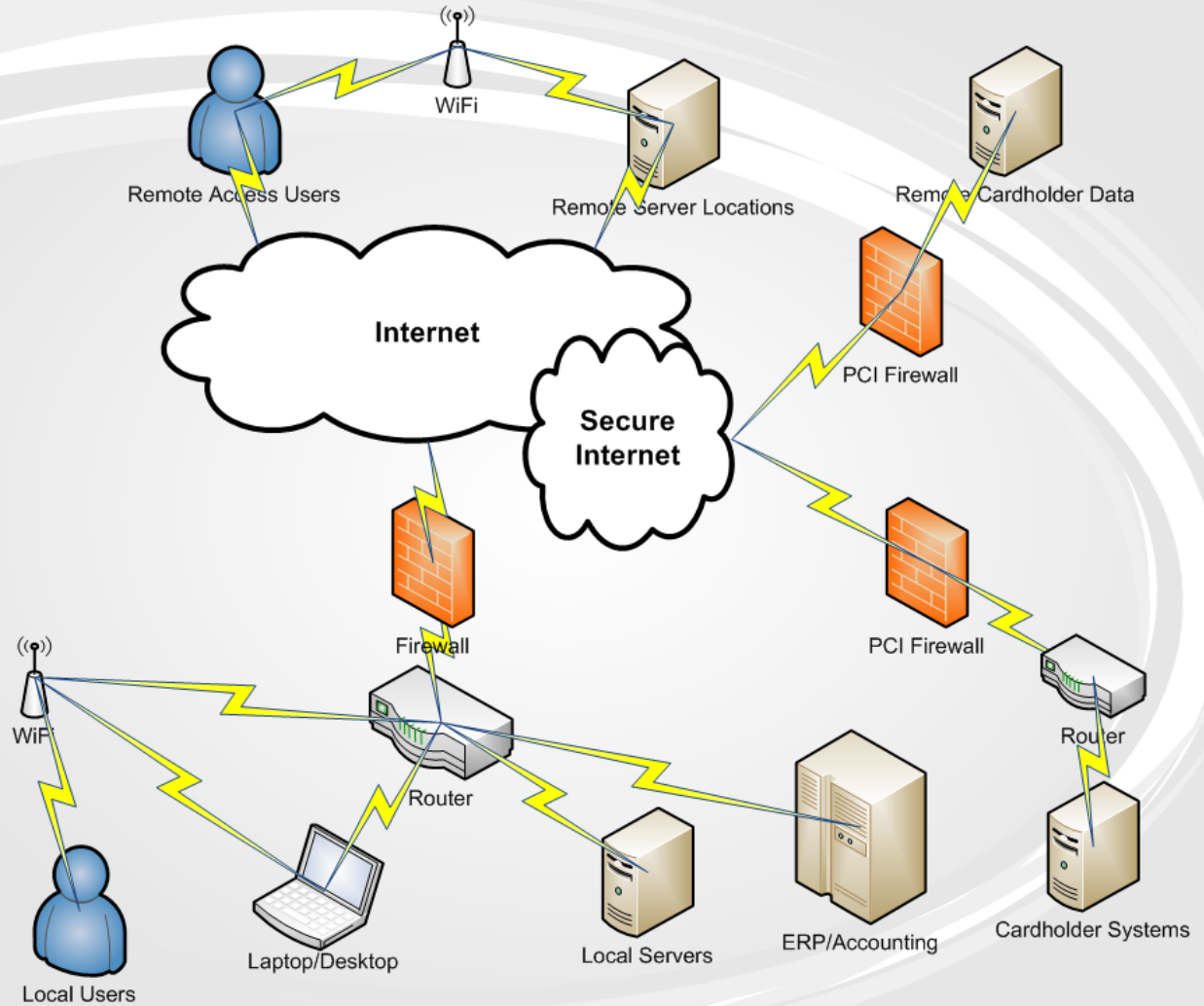
- ❑ Two factor authentication
 - Something you have
 - Something you know
 - Tokens/Smartcards
- ❑ Maintain unique logon
 - Easy for you, easy for a hacker
 - No sharing – every one should have a unique logon and password
 - Vendors/Partners





The Fifth Deadly Sin: Sin of Gluttony

What is a "Flat" Network?





Sin of Gluttony

Separate Network

Firewall to separate network traffic

Approval to allow specific traffic by port and protocol

Identify Systems

Separate applications and systems

Reduce Scope

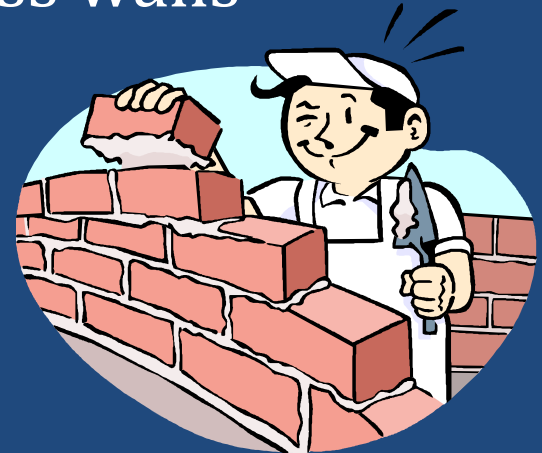
Minimize risk
Minimize data
Minimize number of applications



The Sixth Deadly Sin: Sin of Pride

Poor Perimeter Defense

- Point of attack – build the fortress walls
 - Implement a firewall
 - Hardware vs. software
- Automate
 - Intrusion Detection Service (IDS)
 - Intrusion Prevention Services (IPS)
 - Automate notifications of attacks
 - Collect and review log data





The Sixth Deadly Sin: Sin of Pride

- Review remote access
 - Two factor authentication
 - Remote administration requirements
 - Who has to have access?
 - Convenience versus requirement
 - Vendor/Partner access
 - Assess the risk
 - Limit the access
 - Separate log on accounts for maintenance





The Seventh Deadly Sin: Sin of Accessibility

Wi-Fi for everyone

- Identify business requirement for wireless
 - Separate the networks
 - Payment/Cardholder applications
 - PA-DSS Certification
 - Resources
- Create a security plan
 - Wi-Fi Security
 - Access point management
 - Rogue detection





The Seventh Deadly Sin: Sin of Accessibility

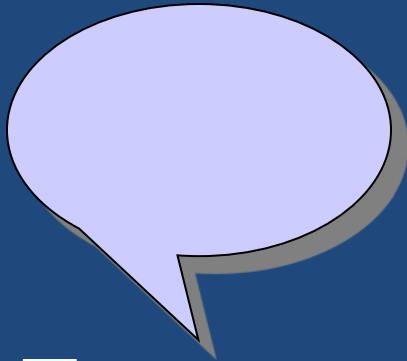
- ❑ Encrypt, encrypt, encrypt
 - Encrypt the tunnel
 - Encrypt the access
 - Encrypt the payload





The Seven Deadly Sins of PCI Compliance

QUESTIONS AND COMMENTS



- ▣ Questions?
- ▣ Comments?
- ▣ Thank You!

The information in this presentation is based on the personal experience and opinions of the presenters. References herein are used without permission and should not be reproduced or used for commercial purposes. Such references include material from the PCI Security Standards Council Data Security Standards, MasterCard International, Visa, Inc., Morgan Stanley Discover & Co., and American Express Company.