Cal Poly PCI DSS
Compliance Training and Information

Training Objectives

- Understanding PCI DSS
  - What is it?
  - How to comply with requirements
- Appropriate ways to handle payment cards
  - Protecting cardholders & Cal Poly

Agenda

- Part 1: PCI DSS Compliance Basics
- Part 2: PCI DSS Driving Factors
- Part 3: Securing PCI Data – Why and How?
- Part 4: Review

Part 1

PCI DSS Compliance Basics

What is PCI DSS?

PCI DSS =

Payment Card Industry Data Security Standard

- The result of a collaboration between Visa, MasterCard, American Express, Discover, and JCB to create common industry security requirements.
- Provides a baseline of technical and operational requirements designed to protect cardholder data.
- Compliance is mandated for all organizations handling credit card data.

A Brief History of PCI DSS

- 2000 – Visa introduces cardholder information security program (CISP) for the USA
- 2001 – Visa Mandates CISP for all merchants
- 2000 – 2004: Other Card companies follow suit with their own programs (i.e. MasterCard's SDP program, Amex DSOP program, etc.)
- 2004 – Payment Card Industry (PCI) announces the Data Security Standard (DSS)
- 2005 – Card Brands begin mandating compliance with PCI DSS
- 2006 – PCI Security Standards Council is formed and PCI DSS v1.1 is released
- 2007 – New compliance deadlines set for Level 1 and Level 2 merchants
- 2007 – **Fines** for non-compliance, starting 10/1/07 for **Level 1** and 1/1/08 for **Level 2**
- 2008 – Visa issues Payment Application Security mandates with associated deadlines for compliance
- 2009 – October, 2008: PCI DSS v1.2 is released
- 2009 – **Fines** for non compliance implemented for **Level 3** merchants
- 2009 – MasterCard announces that, effective June 30, 2011, all **Level 1** and **Level 2** merchants doing an internal audit or self assessment will need to have staff attend SSC sponsored PCI DSS training and maintain appropriate certifications
- 2010 – October, 2010: PCI DSS v2.0 is released

PCI Terms

- **Payment cards** – credit cards, debit cards, and other cards that facilitate cardholder payments
- **Card present transactions** – the cardholder presents the actual card to the merchant for processing. Usually swiped into a register or terminal and a signature is obtained.
- **Card not-present transactions** – the cardholder gives his/her payment card information over the phone or sends his/her card information on a designated form. A form may include a signature, however, signatures are usually not obtained for this type of transaction.

PCI Data Fields - What can never be stored!

What the PCI Rules Say About Data Storage

	Data Element	Storage Permitted	Protection Required	Rule 3.4 Applies[1]
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardholder Name[2]	Yes	Yes[2]	No
	Service Code[2]	Yes	Yes[2]	No
	Expiration Date[2]	Yes	Yes[2]	No
Sensitive Authentication Data[3]	Full Magnetic Stripe	No	n/a	n/a
	CVC2/CVV2/CID	No	n/a	n/a
	PIN/PIN Block	No	n/a	n/a

[1]Requires rendering the PAN unreadable through encryption, truncation, or other means.
[2]Must be protected if stored with PAN.
[3]Must not be stored after authorization, even if encrypted. *Source: PCI Security Standards Council*

What are the Requirements?

- PCI DSS is comprised of 12 high-level requirements, which includes over 200 sub requirements (!)
  - https://www.pcisecuritystandards.org/security_standards/index.php
- Requirement 12.6.1 is the mandate to educate personnel who handle credit cardholder information upon hire and at least annually. In other words, the reason for this training. . .

PCI Data Security Standard (DSS)

12 High-Level requirements – deceptively simple

Build and Maintain a Secure Network	**Implement Strong Access Control Measures**
Requirement 1: Install and maintain a firewall configuration to protect data **Requirement 2:** Do not use vendor-supplied defaults for system passwords and other security parameters	**Requirement 7:** Restrict access to 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
Protect Cardholder Data	**Regularly Monitor and Test Networks**
Requirement 3: Protect stored data **Requirement 4:** Encrypt transmission of cardholder data and sensitive information across public networks	**Requirement 10:** Track and monitor all access to network resources and cardholder data **Requirement 11:** Regularly test security systems and processes
Maintain a Vulnerability Management Program	**Maintain an Information Security Policy**
Requirement 5: Use and regularly update anti-virus software **Requirement 6:** Develop and maintain secure systems and applications	**Requirement 12:** Maintain a policy that addresses information security

What is in scope for PCI requirements?

- All personnel with access to cardholder data.

- All system components that capture, store, process, or transmit cardholder data. This includes servers, workstations, network devices, and applications, along with anything on the same network segment.

Common PCI DSS Myths

1. **One vendor or product will make us compliant.**
   - PCI DSS compliance is a layered process.
2. **Outsourcing card processing makes us compliant.**
   - Not always (!)
3. **We have completed an SAQ, therefore we are compliant.**
   - PCI DSS compliance is an ongoing process.
4. **We don't take enough credit cards to have to be PCI compliant.**
   - PCI DSS compliance is required for any business that accepts payment cards – even if the quantity of transactions is just one.

The Real Story

PCI DSS is an “All or Nothing” Standard

A single requirement not being met = Non-compliance

How is PCI Enforced?

Card Brands

Card brands have contracts with banks requiring them to ensure their merchants are PCI compliant

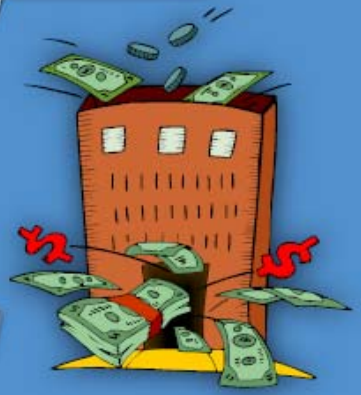
Acquirers

Banks must sponsor Level 1 Service Providers and must then monitor their compliance status

Banks have contracts with merchants requiring them to stay PCI compliant

Merchants

Merchants have contracts with Service Providers requiring them to protect cardholder data



Service Providers

PCI DSS Compliance Implications

- PCI DSS compliance is clear in definition and being enforced by the card brands.
- PCI DSS non-compliance can result in consequences that have dramatic impact on your business.
- Significant fines for non-compliance have been added by the major card brands as of October 1, 2007.

Fines Issued for PCI Non-Compliance

Visa Fines being Levied

Non-Compliance Fines:

- Level 1 Merchant: $25K/mo ($300K/yr) plus tiered merchants bumping down one tier (total $$$ unknown)
- Level 2 Merchant: $5K/mo ($60K/yr)

Breach-Related Fines:

- Failure to report compromise - $100,000
- Egregious violation - $500,000
- Storing full track data (magnetic stripe)
  - $50,000 initial fine
  - $100,000 monthly until issue is resolved

MasterCard Fines being Levied

Quarterly Non-Compliance Fines, As Follows:

- Levels 1 & 2: $25K first quarter; $50K second quarter; $100K third quarter; $200K fourth quarter.
- Level 3: $10K first quarter; $20K second quarter; $40K third quarter; $80K fourth quarter.

Part 2

What's Driving this Whole PCI DSS Thing?

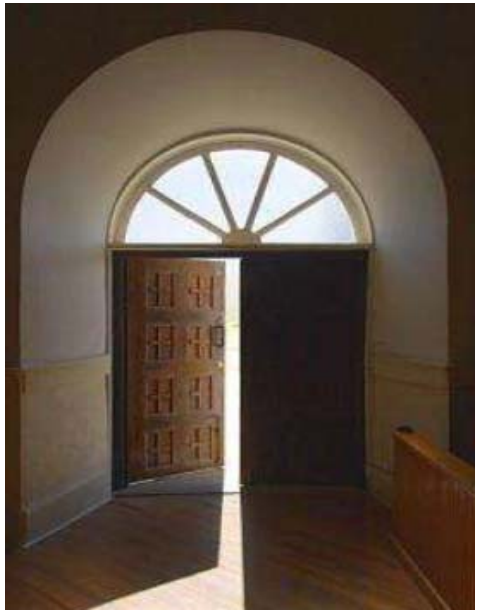
Business Drivers Behind PCI DSS

- Recognize organizational benefits
- Improve operational efficiencies
- Avoid potential breach fines or non-compliance fees
- Achieve Safe Harbor[1] status – consequences waived
- Maintain ability to continue processing credit cards
- Avoid cost of data breach
- Reduce risk – "Hacking" has become a profitable line of business for organized crime

[1]Safe Harbor status: Per Vista, Safe harbor Status requires that "A member, merchant, or service provider must maintain full compliance at all times, including at the time breach as demonstrated during the forensic investigation."

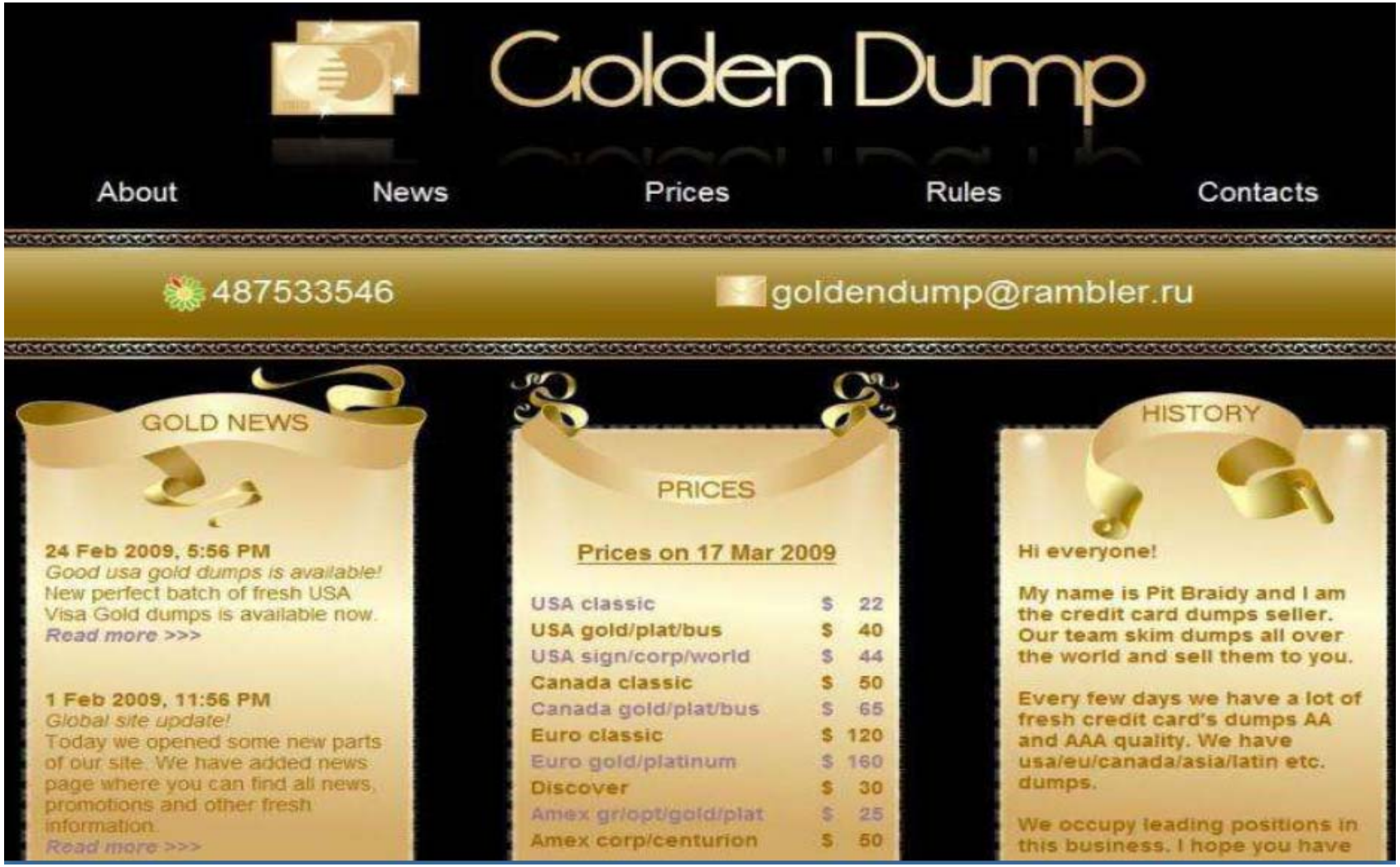
PCI Vulnerabilities Exist at Many Levels

- Vulnerabilities in information security leave open doors for theft
- Vulnerabilities may appear almost anywhere in the credit card processing ecosystem[1]:
  - Point of Sale Devices
  - Desktops/ Laptops
  - Servers
  - Wireless hotspots
  - Web shopping applications
  - Paper-based storage systems
  - Unsecured transmission of cardholder data
  - Unsecured transmission of cardholder data to service providers



[1]PCI Security Standards counsel (SSC) Data Security Standards (DSS) Quick reference Guide

Credit Cards are Being Sold on the Internet



Credit Card Data Beach Chronology

Year(s)	Name of breached Entity	# of Credit Cards Compromised	Impact
2003	Data Processors Intl	5 Million	
2003-2004	BJ's Wholesale	9.2 Million	
2005	DSW Shoes	1.5 Million	
2005	Cardsystems Solutions	40 Million	Card processing right revoked. Went out of business as a result
2007	Dai Nippon	8.6 Million	
2007	Fidelity (Certegy)	8.5 Million	
2007	Hannaford Brothers	4.2 Million	Had to spend "millions" on security upgrades
2005-2008	TJX Companies	54.7 Million	Estimated total losses = $ 256M- 4.5B
2008-2009	RBS World	1.5 Million	Estimated cost $90M
2009	Heartland payment Solutions	130 Million	Related Expenses total $140 M so far…
2011	Sony	24.6 Million	Estimated cost $171 Million

Part 3

Securing PCI Data
Why and How?

The Challenge…

Ironically, the things that make our life easier and more convenient also make crime easier and more convenient.

Ongoing Campus PCI Efforts

- Quarterly computer scans
- Annual employee and student employee training of PCI policies and security awareness
- Annual network penetration testing
- PCI DSS Assessment and report of compliance self-assessment questionnaire
- (SAQ) form completion

6 Main Goals of PCI-DSS

- Build and maintain a secure network
- Protect cardholder data
- Maintain a Vulnerability Management Program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an Information Security Policy

Meeting Our Goals

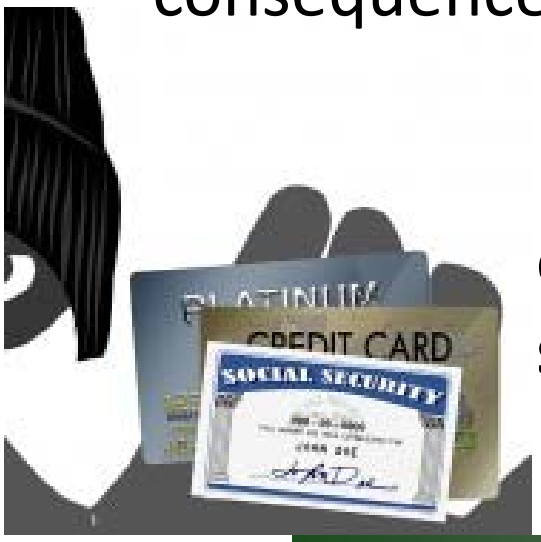
- Maintain a secure network through strong passwords
- Protect Cal Poly confidential data and your personal information
- Don’t email confidential information
  - Don’t respond to phishing messages
- Practice safe Web surfing
  - Don’t respond to pop-up hoaxes
- Comply with physical security policies and procedures.

Use Strong Passwords

- Store your passwords encrypted.
- Keep your password private, don't share it with co-workers.
- No one at Cal Poly will ask you for your password.
- Your bank or any reputable company will never solicit this information.
- If you are ever asked for your password in an email or over the phone – don't give it out.

Protect Cardholder Data

As a custodian of customer information, it is your role to protect cardholder data. If cardholder data is compromised, the owner of the information suffers the consequences, whether financial or by reputation. Cal Poly will ultimately face the same consequences.



If you wouldn't *hand* a stranger your own credit card, then don't hand them someone else's!

Phishing Email

- Be wary of suspicious email messages.
- Don't open email attachments unless you are expecting them.
- E-mails may include viruses or misleading links to web pages which ask for personal information.
- Don't click on URLs that people send you unless it is a known "safe" site.
- Report suspicious email to abuse@calpoly.edu.

Website Safety

- Malicious websites can be infected with spyware or malware and can infect your computer when you visit them.
  - Stay away from unknown sites or sites that anti-virus software warns against.
- Be aware of “pop-ups” that could contain spyware.
- Use known sites that are secure “https” for personal business.
- Spyware and malware could allow an opening to steal confidential information.

It's Not Only Electronic Data

- Protect information in all its forms.
- Keep printed confidential information out of site.
- Use locks on cabinets and offices appropriately.
- Shred documents when they are no longer required.
- When speaking about a confidential matter, be sure that your conversation will not be overheard.

Primary Guiding Principle for Cardholder Data

If you don’t absolutely need to store it, DON’T!

Part 4

We ALL Have a Role to Play to Comply with PCI DSS.

Review

- The industry has mandated PCI DSS compliance with fines for non-compliance.
- PCI-DSS regulations applies to everyone who accepts credit cards.
- Credit card fraud is a serious problem.
- Compliance with PCI DSS helps alleviate vulnerabilities and protect cardholder data.

Ways to Protect Cardholder Data

- Never share your password with anyone!
- Keep your desk clear of any sensitive materials.
- Always properly dispose of paper records with cardholder data, using cross-cut shredders or approved shredding bins.
- Don’t allow unauthorized individuals around PCI devices.
- Be alert! If you’re unsure about what could be a security risk, ask your supervisor.

Helpful Resources

Learning about information security and safe computing need not be a daunting task. There are resources on campus to help you:

- Cal Poly Information Security Website
  - http://www.security.calpoly.edu/
- Cal Poly Information Technology Services – Service Desk
  - http://www.servicedesk.calpoly.edu/
- PCI Security Standards Council
  - http://www.pcisecuritystandards.org

References: Some content contributed by Halock Security Labs (Halock.com)