




ISACA HAWAII
PCI v2.0: Is Your Organization Prepared to Meet the New Requirements?




March 25, 2011



James Cowing
CISSP, PCI-QSA, PA-QSA, CISM
CEO
Digital Resources Group



Course Objectives



What you will learn:

- Who must comply with PCI DSS 2.0 and by when?
- What are the key requirements of PCI DSS and the latest updates of version 2.0?
- What strategies can be used to deal with PCI DSS 2.0 compliance challenges?
- How can PCI DSS 2.0 be used as a springboard to strengthen a company's overall data security posture and/or your governance program?
- How can your company simplify the effort and minimize the cost of complying with PCI DSS 2.0?

©2011 Digital Resources Group 2



DRG PCI Services




- ✓ Qualified Security Assessor (QSA)
- ✓ Approved Scan Vendor (ASV)
- ✓ Payment Application Qualified Security Assessor (PA-QSA)

Full-service consultative and technical security support solutions since 1997:

- Security assessment & consultation
- Compliance validation (PCI, HIPAA, SOX)
- Merchant Security Education & Training
- Remediation
- Implementation
- Incident response
- Security product solutions
- Related security support services

DRG has performed hundreds of PCI assessments for industry-leading companies

©2011 Digital Resources Group 3



Section I

IMPORTANCE OF DATA SECURITY

©2011 Digital Resources Group 4



Data Breaches Don't Happen Here!?




UH computer breach may have compromised 53,000 people

July 06, 2010

More than 53,000 people, who did business with the University of Hawaii at Manoa parking office's data base from 1998-2009, are being notified by mail that they may be affected by a computer security breach. The FBI and Honolulu Police Department are investigating the breach that was discovered on June 15 during a routine audit. University officials say the unauthorized access to a computer server used by the Manoa parking office occurred on May 30. Affected are 53,000 records, which included 41,000 Social Security numbers and 200 credit card numbers.

©2011 Digital Resources Group



2010 Data Breach Analysis

Data at Risk

Category	Percentage
Payment Card Data	85%
Sensitive Company Data	3%
Intellectual Property	2%
Other	12%

Targeted Assets

Category	Percentage
Software POS	75%
E-Commerce	9%
Employee Workstation	11%
Payment Processing	3%
Other	2%


Source: SpiderLabs 2011 Global Security Report

©2011 Digital Resources Group 6

DRG

Top Risks to Hawaii Companies

Costly PCI Mistakes:
Storing Track, CVV or PIN Data
Not Encrypting, Masking PANs, etc.



Common Causes of Card Data Exploits:

1. Web applications and poor coding practices
2. Data retention and archival practices
3. Reliance on 3rd Parties (cash register co, etc.)
4. Poor network design
5. Lack of security policies and employee education

©2011 Digital Resources Group 7

DRG

Measuring Impact from a Security Breach



- Customer Financial Loss (\$\$\$ impact)
- Loss of **customer loyalty** and brand impairment
- Call volumes, **Media & Press**
- Forensic investigation cost
- Impacted **customer notification**
- **Lost employee productivity**
- Financial statement and stock values
- **Litigation** and restitution costs
- Card brand and regulatory **fin**es
- New security & audit requirements

©2011 Digital Resources Group 8

DRG

Section II

PCI SECURITY STANDARDS COUNCIL (SSC)

©2011 Digital Resources Group 9

DRG

PCI Security Standards Council

- Payment Card Industry Data Security Compliance Initiative
 - Five major card brands unite for Common Security
 - Card Brands security started in 2001; PCI formed in 2004
 - First PCI DSS was released in 2006
 - Current Data Security Standard (DSS) – version 1.2 / 2.0
- Enforced by **Banks** (Acquirers, AMEX and Discover)

©2011 Digital Resources Group 10

DRG

PCI Security Initiatives Broaden

©2011 Digital Resources Group 11


DRG

Who does PCI Apply to?

- **Applies to all who Store, Process or Transmit Card Data**
 - Card-Present (CP)
 - Dial-up and Paper
 - Ecommerce and Websites (CNP)
 - Mail /Telephone Order (MOTO)
 - Fax and other payment mechanisms

Card Associations' Goal: Global Mass Adoption


©2011 Digital Resources Group 12



Payment Brand Compliance Programs

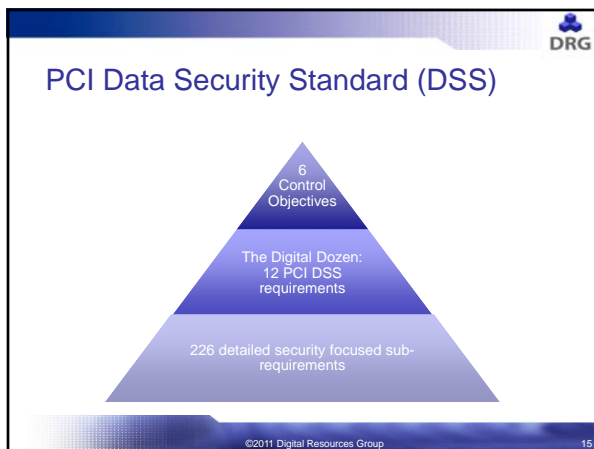
Level	Visa USA	MasterCard	Discover	AmEx
1	Merchants processing over 6 million Visa transactions annually, identified by another payment card brand as Level 1, or merchants compromised in last year.	Merchants processing over 6 million MasterCard transactions (all channels) annually, or compromised merchants	Merchants are currently not categorized into levels based upon transaction volume. Discover takes a risk based approach to validating compliance.	Merchants processing over 2.5 million American Express Card transactions annually
2	Merchants processing 1 million to 6 million Visa transactions annually	Merchants processing over 150,000 MasterCard e-commerce transactions annually		Merchants processing 50,000 to 2.5 million American Express transactions annually
3	Merchants processing 20,000 to 1 million Visa e-commerce transactions annually	Merchants processing over 20,000 MasterCard e-commerce transactions annually		Merchants processing less than 50,000 American Express transactions annually
4	Merchants processing less than 20,000 Visa e-commerce transactions annually, and all other merchants processing up to 1 million Visa transactions annually	All other MasterCard merchants		N/A

©2011 Digital Resources Group 13



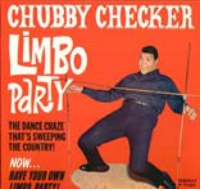
Section III PCI DSS GOALS AND REQUIREMENTS

©2011 Digital Resources Group 14



DRG

On-Site Audits - Mid Year Changes Impact Level 2 Merchants



MasterCard and Card Brands are lowering the bar...

As of July 1, 2011 all Level 2 merchants will be required to complete an On-site Audit.

©2011 Digital Resources Group 19

DRG

Section IV PCI DSS LIFECYCLE, TIMELINES AND UPDATES


©2011 Digital Resources Group 20

DRG

PCI DSS Lifecycle Improves

NEW STANDARDS PUBLISHED

- Major new releases of PCI DSS and PA-DSS disclosed in October 2010.
- Lengthens 3-year lifecycle
- Previous versions remain effective for 14 months



©2011 Digital Resources Group 21

DRG

PCI DSS 2.0 Lifecycle

- Version 2.0 published Oct. 28, 2010
- Effective January 1, 2011
- DSS 2.0 required Jan 2012
- Existing version 1.2.1 retires December 31, 2011
- Most SAQs starting DSS 2.0
- Next PCI Update & Feedback begins November, 2011

©2011 Digital Resources Group

22

DRG

Drivers for Change

- Provide greater clarity on PC DSS and PA-DSS
- Improve flexibility
- Help manage evolving risks / threats
- Align with changes in industry best practices
- Clarify scoping & reporting
- Eliminate redundant sub-requirements

©2011 Digital Resources Group

23


DRG

PCI 2.0 or 1.2? The Choice Is Yours *(for now)*

- Version 2.0 is not effective until Jan. 1, 2011, after which time it will exist in parallel with the current version—1.2.
 - That means for all of 2011 retailers will have the option of using either version to validate their compliance.


©2011 Digital Resources Group

24




Section V
**PCI DSS v1.2
 LIFECYCLE 2009 - 2011**

©2011 Digital Resources Group 25




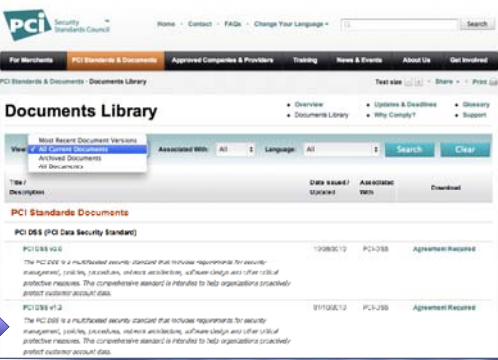
PCI DSS v1.2.1 Overview



- **Timeline:**
 - Released July 2009
 - Retired December 31, 2011
- **Updates from v1.1 to v1.2:**
 - Provides greater clarity on PCI DSS requirements
 - Offers improved flexibility
 - Manages any evolving risks and threats
 - Incorporates existing and new best practices
 - Clarifies scoping and reporting
 - Eliminates redundant sub-requirements
 - Consolidates documentation

©2011 Digital Resources Group 26

https://www.pcisecuritystandards.org/security_standards/documents.php

Documents Library

Doc #	Description	Doc Issue/Version	AM/OS/MS/WH	Download
PCI DSS v1.2	The PCI DSS is a multistep security standard that includes requirements for security management, controls, processes, network architecture, software design and other critical protective measures. The comprehensive standard is intended to help organizations proactively protect customer account data.	07/2009/12	PCI-DSS	Agreement Required
PCI DSS v1.1	The PCI DSS is a multistep security standard that includes requirements for security management, controls, processes, network architecture, software design and other critical protective measures. The comprehensive standard is intended to help organizations proactively protect customer account data.	07/2006/12	PCI-DSS	Agreement Required

©2011 Digital Resources Group 27

DRG

Section VI


PCI DSS v2.0 UPDATES – PREPARING FOR THE FUTURE

©2011 Digital Resources Group 28

DRG

At-a-Glance – Key Updates

- Scoping
- Logging
- Risk-based approach
- Alignment between PA-DSS & PCI-DSS
- Recognition of small merchant environments
- New website and updated supporting documentation




©2011 Digital Resources Group 29

DRG

PCI DSS v2.0 Updates

Requirement Impact	Reason for Change	Proposed Change	Category
PCI DSS Intro	Clarify Applicability of PCI DSS and cardholder data.	Clarify that PCI DSS Requirements 3.3 and 3.4 apply only to PAN. Align language with PTS Secure Reading and Exchange of Data (SRED) module.	Clarification
Scope of Assessment	Ensure all locations of cardholder data are included in scope of PCI DSS assessments.	Clarify that all locations and flows of cardholder data should be identified and documented to ensure accurate scoping of cardholder data environment.	Additional Guidance
PCI DSS Intro and various requirements	Provide guidance on virtualization.	Expanded definition of system components to include virtual components. Updated requirement 2.2.1 to clarify intent of "one primary function per server" and use of virtualization.	Additional Guidance


©2011 Digital Resources Group 30



PCI DSS v2.0 Updates, Con't.

Requirement Impact	Reason for Change	Proposed Change	Category
PCI DSS Requirement 1	Further clarification of the DMZ.	Provide clarification on secure boundaries between internet and card holder data environment.	Clarification
PCI DSS Requirement 3.2	Clarify applicability of PCI DSS to issuers or issuer Processors.	Recognize that issuers have a legitimate business need to store Sensitive Authentication Data.	Clarification
PCI DSS Requirement 3.3	Clarify key management processes.	Clarify processes and increase flexibility for cryptographic key changes, refresh or replace keys, and use of split control and dual knowledge.	Clarification


©2011 Digital Resources Group 31




PCI DSS v2.0 Updates, Con't.

Requirement Impact	Reason for Change	Proposed Change	Category
PCI DSS Requirement 6.2	Apply a risk based approach for addressing vulnerabilities.	Update requirement to allow vulnerabilities to be ranked and prioritized according to risk.	Evolving Requirement
PCI DSS Requirement 6.5	Merge requirements to eliminate redundancy and Expand examples of secure coding standards to include more than OWASP.	Merge requirement 6.3.1 into 6.5 to eliminate redundancy for secure coding for internal and Web-facing applications. Include examples of additional secure coding standards, such as CWE and CERT.	Clarification
PCI DSS Requirement 12.3.10	Clarify remote copy, move, and storage of CHD.	Update requirement to allow business justification for copy, move, and storage of CHD during remote access.	Clarification

©2011 Digital Resources Group 32



DSS v2.0 vs. Current v1.2 Cardholder Data Storage Clarification



Full Magnetic Stripe or Track Data

Card Verification Value (CVV) - CVC2 / CVV2

	Data Element	Storage Permitted	Render Stored Account Data Unreadable per Requirement 3.4
Account Data	Primary Account Number (PAN)	Yes	Yes
	Cardholder Name	Yes	No
	Service Code	Yes	No
	Expiration Date	Yes	No
	Full Magnetic Stripe Data?	No	Cannot store per Requirement 3.2
Sensitive Authentication Data	CVV2/CVC2/CVV2/CID	No	Cannot store per Requirement 3.2
	PIN/PIN Block	No	Cannot store per Requirement 3.2

©2011 Digital Resources Group 33

DRG

DSS v2.0 vs. Current v1.2

Network Diagram/Scoping Clarification

PCI DSS Requirement 1.1.2
Current network with all connection to cardholder data including any wireless networks

- The drawing must include **all Cardholder Data Locations** and a **flow of Cardholder Data** through the network
- The drawing must show if a **wireless network is used** and if Cardholder Data flows over the wireless network
- The diagram must be **dated** and **current**

Can you find the non-compliant requirement in this drawing?

©2011 Digital Resources Group 34

DRG

DSS v2.0 vs. Current v1.2

Outbound Traffic from CDE to IPs Outside DMZ (1.3.5)

- DSS v1.2 indicates no room to have any outbound connection from CDE to IPs outside DMZ (even of legitimate reasons like transmitting encrypted information from one network to another over SSL port 443).
- DSS v2.0 allows merchants to have outbound access open as long as there is legitimate reason and the access has been explicitly authorized by the merchant.

©2011 Digital Resources Group 35

DRG

DSS v2.0 vs. Current v1.2

One Primary Function per Server and Virtualization (2.2.1)

- DSS v1.2 the requirement was to implement only one primary function per server.
 - It was not clear in a virtualized environment if two virtual machines (VMs) running on the same physical hardware box was considered as two primary functions per 'server'
- DSS v2.0 the council makes it easy by saying that in virtualized environments you can have multiple VMs on same physical box as long as each image implements one primary function
 - Clarification - you can have a VM for a webserver and a VM for a database server running side by side but you can't have one VM with a webserver and database server on the same image

©2011 Digital Resources Group 36

DRG

DSS v2.0 vs. Current v1.2

Assign risk ranking to vulnerabilities - Internal scanning (6.2)

- DSS requires merchants to have a vulnerability management program in place to identify and fix vulnerabilities discovered in the cardholder data environment (CDE)
 - DSS v1.2 the merchants were required to patch and rescan internal networks until 'passing results are obtained'
 - DSS v2.0 requires that merchants come up with a risk ranking for these vulnerabilities based on industry best practices like CVSS (this is a requirement after June 30, 2012)

©2011 Digital Resources Group 37

DRG


Section VII

PA DSS GOALS AND REQs

©2011 Digital Resources Group 38

DRG


PA-DSS Goal



Develop secure payment applications that do not store prohibited data, such as full magnetic stripe, CVV or PIN data, and ensure vendor payment applications support compliance with PCI DSS.

"Payment applications should facilitate, and not prevent, the customer's PCI DSS compliance."
-PA-DSS Program Guide


©2011 Digital Resources Group 39



Who Does PA-DSS Apply To?

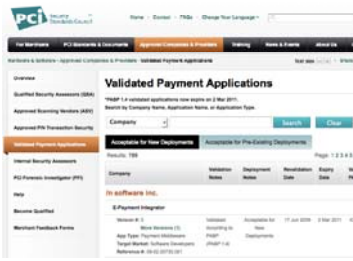
- Directly
 - Payment Application Providers
 - QSAs and PA-QSAs
- Indirectly
 - Merchants who buy payment applications
 - Service providers who buy payment applications

©2011 Digital Resources Group 43



PCI Validated Payment Applications

- Merchants responsibility to use compliant apps
- Insist your vendors offer PA-DSS protection
- Compliant applications on PCI SSC web site
- Non-compliant apps no longer permitted by acquirers after 10/09



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

©2011 Digital Resources Group 44



Section VIII

PCI AS A SPRINGBOARD TO STRENGTHEN DATA SECURITY AND GOVERNANCE PROGRAMS

©2011 Digital Resources Group 45

DRG

PCI vs. Other Standards and Frameworks

PCI best foundation for IT Governance:

- Specific Requirements for "Controls in Place"
- Detailed Examination and Testing Procedures
- Structured Template for Report on Compliance

©2011 Digital Resources Group ©2008 Digital Resources Group

DRG

PCI Promoted from an IT Project to Pillar of GRC

Governance, Risk, Compliance

SOX GLBA ISO 17799 PCI HIPAA SAS 70 NERC

Policies Access Controls User Provisioning Data Protection Network Infrastructure Identity Management Monitoring


©2011 Digital Resources Group ©2008 Digital Resources Group

DRG


PCI Role Evolves within GRC

- Controls:** Migrate from annual single IT initiative to ongoing business processes
- Lifecycle:** Build security in earlier and throughout the Business and Systems lifecycle
- Ongoing:** Continuous security testing, improvement and optimization
- Compliance:** Manage and streamline competing audit requirements

©2011 Digital Resources Group ©2008 Digital Resources Group




Modify PCI to Meet Your Requirements



- PCI controls framework, built on ISO 17799 standard, can be modified to meet your particular business and risk requirements
 - Threat vectors
 - Data elements and data classification types
 - Asset and resource inventories
- Confidential data elements tailored to your business
 - Personally identifiable information
 - Social security number
 - Drivers license
 - Banking information
 - Mother's maiden name
 - Date of birth
 - Healthcare records

©2011 Digital Resources Group ©2008 Digital Resources Group



Section IX

HOW TO MAKE COMPLIANCE EASIER

©2011 Digital Resources Group 50




PCI DSS Compliance is Daunting




- Onsite audit: 50 pg Security Audit Procedures; > 240 separate compliance test requirements
- Interviews, auditor observations, site visits, network and systems testing
- Scope: data centers, corporate offices, call centers, partners, offsite storage, etc. (where applicable)
- Substantial resources and time intensive
- "More comprehensive than other IT audits"
 - (such as SOX, GLBA, HIPAA, etc.)
- Extensive documentation and policies required
- No one passes first time – Most customers grossly underestimate the effort to compliance

The right tools and technology partners are essential for success

©2011 Digital Resources Group 51




PCI Process - Steps for Success




- Define Card Process Flow
- Identify Card Processing Environment
- Network Architecture / Design Walk-Thru
- Scope – Network, Assets, Departments
- Network segmentation
- POS Systems
- Card data retention and archiving
- Data Encryption Requirements
- Third Party Relationships

©2011 Digital Resources Group 52




Role of Network Segmentation




- Reducing the scope can save time and \$\$\$
- Define the Card Processing Environment
 - Production vs. Dev., Data Center, Corporate Offices
 - SAN, Offsite Media Storage
 - Customer Care or Phone Center
 - Third Party Providers, Hosting Locations
- Segmentation Tools: VLANs, ACLs, Firewalls

©2011 Digital Resources Group 53



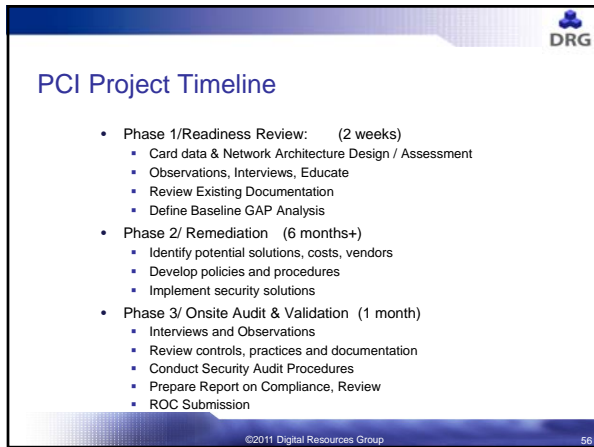
Role of QSA

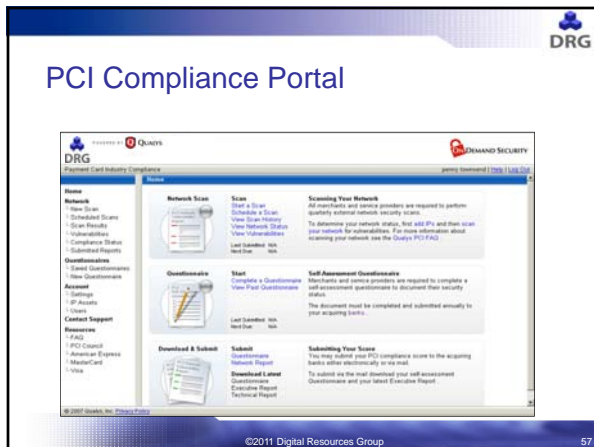


- Trained and credentialed card security experts
- Ensures Customer's implementation meets PCI security requirements
- Makes recommendations based on unique circumstances/needs
- Recommends solutions or providers to facilitate compliance
- Guide your clients to become fully PCI compliant

©2011 Digital Resources Group 54

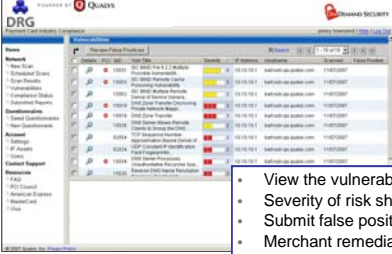






DRG

Review Vulnerabilities



- View the vulnerabilities
- Severity of risk shown
- Submit false positives or exceptions
- Merchant remediates
- Re-Scan target hosts to validated




©2011 Digital Resources Group 58

DRG

Dial-Up vs. Internet Connected Merchants

- **Dial-Up Merchants**
 - TurboPCI Workbook
 - PCI Security Policies & Procedures

- **Internet Connected Merchants**
 - Quarterly Network Scans
 - TurboPCI Workbook
 - PCI Security Policies & Procedures


©2011 Digital Resources Group 59

DRG

Section X


PCI SSC PRIORITIZED APPROACH

©2011 Digital Resources Group 60




Objectives of a Prioritized Approach

- Prioritize efforts based on the risk associated with handling cardholder data
 - Security efforts can first focus on certain PCI DSS requirements
- Reduce risk associated with account data compromise by:
 - Not retaining magnetic stripe data
 - Minimize and secure storage of PAN
 - Using network segmentation to reduce scope



©2011 Digital Resources Group 61



PCI SSC Validation Tool


Download the Prioritized Approach Tool from
https://www.pcisecuritystandards.org/security_standards/documents.php

PCI DSS Requirements	Milestone				
	1	2	3	4	5
Requirement 1: Install and maintain a firewall configuration to protect cardholder data					
1.1. Document policies for approving and testing all firewall configurations					
1.2. Document rules to allow only authorized traffic and deny all other traffic					
1.3. Document and test firewall rules and configurations for cardholder data, including any wireless networks					
1.4. Document the process for firewall rule changes and updates					
1.5. Document the process for firewall rule testing and updates					
1.6. Document the process for firewall rule testing and updates					
1.7. Document the process for firewall rule testing and updates					
1.8. Document the process for firewall rule testing and updates					
1.9. Document the process for firewall rule testing and updates					
1.10. Document the process for firewall rule testing and updates					

©2011 Digital Resources Group 62




Important Milestones




- If you don't need it, don't store it
- Secure the perimeter
- Secure applications
- Control access to your systems
- Protect stored cardholder data
- Finalize remaining compliance efforts, and ensure all controls are in place

©2011 Digital Resources Group 63




DRG offers TurboPCI Workbook


- The Fastest Way to Turbo Charge Your PCI Compliance at a Low Cost !
- Everything a small merchant needs to build a compliant Retail Business
- Step-by-step easy to understand SAQ instructions
- Full ready to use company PCI Security Policy
- PCI-ready operational forms and templates
- Expansive glossary to define industry terms
- CD-Rom for easy printing of all documents



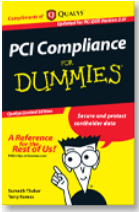
Prices as Low as \$125.00




©2011 Digital Resources Group 67



Or for the Clift Notes references




Bring Your Business Card For a
FREE Copy of the
PCI Compliance for Dummies
Reference Book



Updated for PCI DSS Version 2.0!



©2011 Digital Resources Group 68



Section XII

RECAP

©2011 Digital Resources Group 69


What is required to comply with PCI ?

- Understand your card flow
- Evaluate Risks
- Prioritize Threats
- Identify Compliant Solutions
- If you have questions or need help, engage a QSA (Expert)

Determine Your Compliance Requirements

- Complete an annual SAQ
- Scan regularly (quarterly)
- Reports sent to Acquirer
- Stay Compliant – Protect your Business

©2011 Digital Resources Group 70



Recap and Keys to PCI Success

- Protection of sensitive data is Hawaii Merchant's obligation to the customers served
- Hawaii merchant brand consequences and reputation risk from data breach could be *substantial*
- Financial impact can jeopardize growing concerns
- Verify that your partners and service providers take security as seriously as you do
- Jump on the PCI Compliance bandwagon before too late – risk mitigation measures can provide protection for your brand and your shareholders

©2011 Digital Resources Group 71



Recommended PCI Reading

 **PCI Security Standards Council Website:**
www.pcisecuritystandards.org

 **VISA CISP Website:**
usa.visa.com/merchants/risk_management/cisp.html

VISA PIN Security Website:
usa.visa.com/merchants/risk_management/cisp_pin_security.html

 **Digital Resources Group Website:**
www.drsgf.com

©2011 Digital Resources Group 72

 DRG

Contact Information



James Cowing, CISSP, OSA, PA-OSA, CISM, CPA, CITP
CEO
Digital Resources Group
Data and Network Security Experts
Email: jim.cowing@drgsf.com
Web: www.drgsf.com
Phone: 808-792-1630
Toll Free: 800-559-8120

security assessment • remediation • implementation • incident response • support services

©2011 Digital Resources Group 73
