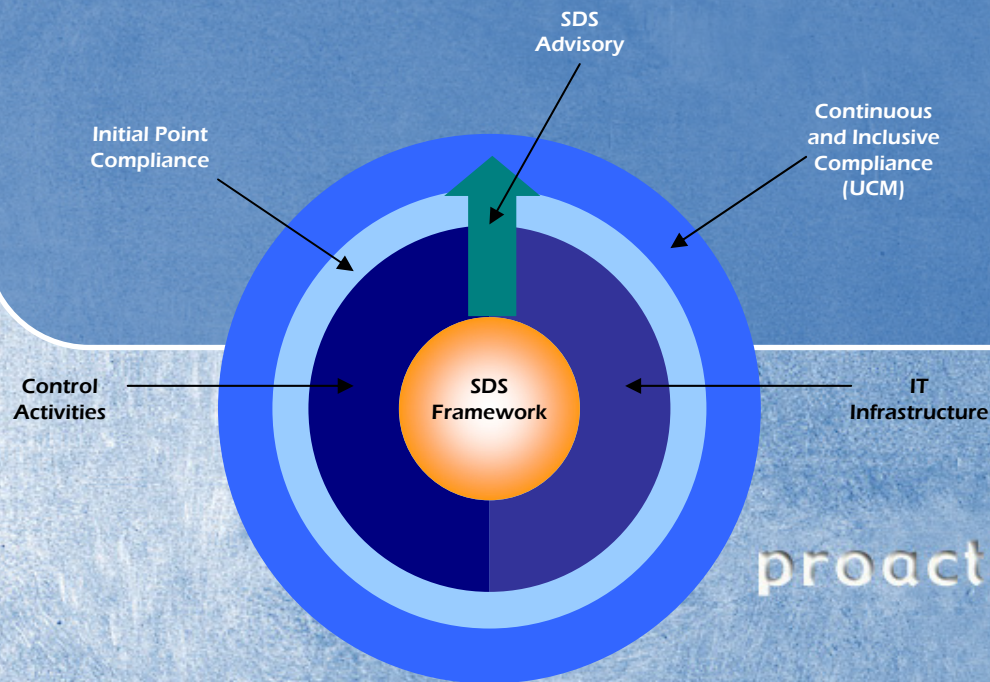


Secure Digital Solutions presents: Safeguarding Data with PCI DSS



proactive > secure > confident

SDS Overview

- Professional consulting services organization with over 10 years experience
- Former clients range from Fortune 50 to mid-size non-public organizations; industries include financial, healthcare, manufacturing, retail and legal services
- Certified and experienced consultants
- Tailored Solutions
- Vendor independent

proactive > secure > confident



PCI DSS – The Beginning

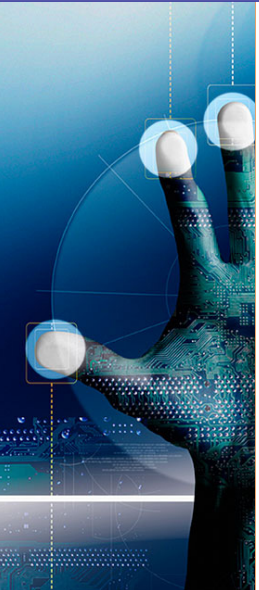
- A business need was discovered to address security controls of confidential electronic information and reduce the loss of revenue due to fraud and theft of financial credit card data.
- PCI originally began as 5 different programs
 - VISA, Mastercard, American Express, Discover and JCB
 - PCI SSC (Payment Card Industry Security Standards Council) formed December 15, 2004
 - PCI Council was established by the original five major credit card companies.
 - PCI Council was designed to manage the ongoing evolution of the Payment Card Industry (PCI) Data Security Standard.

proactive > secure > confident



SDS
SECURE DIGITAL SOLUTIONS

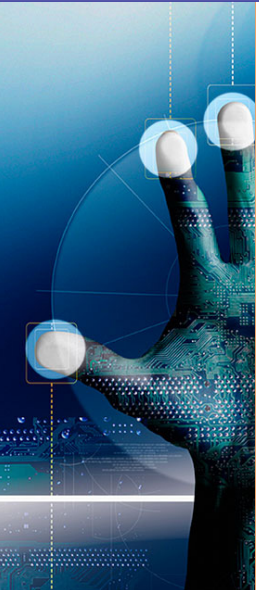
PCI DSS – The Evolution

- 
- PCI DSS 1.0 took effect originally on June 30th 2005
 - PCI DSS version 1.1; after December 31st 2006 version 1.0 was no longer recognized
 - Key changes to version 1.1
 - sub-requirement 10.7 said
 - An audit history usually covers a period of at least one year, with a minimum of 3 months available online.
 - In v1.1, it was stated differently
 - Retain audit trail history for at least one year, with a minimum of three months online availability.
 - Addition of requirement 6.6
 - Ensure that all web-facing applications are protected against known attacks by applying either of the following methods:
 - Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security
 - Installing an application layer firewall in front of web-facing applications.
 - » **Note:** *This method is considered a best practice until June 30, 2008, after which it becomes a requirement.*
 - PCI DSS v1.1 was valid until December 31st, 2008
 - PCI DSS v1.2 was released on October 1st, 2008
 - Seen as an improvement to the standards and not a departure from its' original intent and approach.
 - Makes requirement 6.6 mandatory
 - Adds flexibility in the time frame for review of firewall rules from quarterly to every 6 months.
 - A number of clarifications were issued to address cardholder data in a wireless environment
 - New implementations of WEP are not allowed after March 31, 2009
 - Current implementations must discontinue use of WEP after June 30, 2010
 - States the use of antivirus software applies to all operating system types.
 - The standard now requires companies to visit offsite storage locations annually.
 - It also clarified that secure media applies to electronic and paper media that contains cardholder data.

PCI DSS – The 12 Requirements

- Sections 1 & 2: Build and Maintain a Secure Network
- Sections 3 & 4: Protect Cardholder Data
- Sections 5 & 6: Maintain a Vulnerability Management Program
- Sections 7, 8 & 9: Implement Strong Access Control Measures
- Sections 10 & 11: Regularly Monitor and Test Networks
- Section 12: Maintain an Information Security Policy

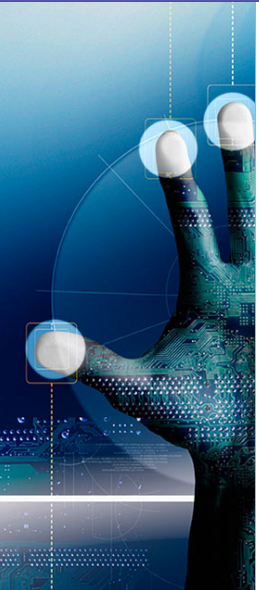
proactive > secure > confident



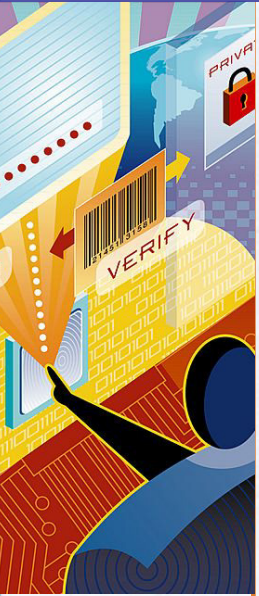
General PCI DSS Merchant Levels

Merchant Level	Criteria	Annual Self Assessment Questionnaire
Level 1	a) Over 6 million transactions per year b) Any merchant with an account compromise c) Any merchant that VISA determines should comply with Level 1 requirements d) Any merchant identified by any other payment card brand as Level 1	SAQ-A
Level 2	1 million to 6 million transactions per year regardless of acceptance channel	SAQ-B

PCI DSS Merchant Levels



Merchant Level	Criteria	Annual Self Assessment Questionnaire
Level 3	Any merchant processing 20K to 1 million VISA e-commerce transactions per year	SAQ-B
Level 4	Fewer than 20K VISA e-commerce transactions per year and all other merchants processing up to 1 million transactions per year.	SAQ-C
Level 5	All other merchants not included above and all service providers defined by a payment brand as eligible to complete a SAQ.	SAQ-D



Advantages to Becoming PCI Compliant

- Increase customer confidence
- Position your business to offer services to high-profile clientele
- Gain accountability around the management of information systems and data access
- Create a competitive edge by positioning your company as a leader in the space by taking a proactive approach to compliance
- Establish a solid baseline for an information security program
- Position your organization as a proactive leader; an organization that takes the security of client data seriously
- Comply with state laws where you are operating

proactive > secure > confident

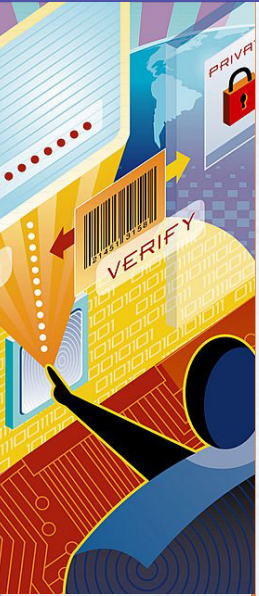
Some Facts about PCI Compliance

- Acquirers (Banks) will be fined \$5,000 to \$25,000 a month for each merchant who does not comply with PCI DSS
 - These fines are passed onto Merchants by the Acquirers
- An estimated 78 percent of consumers will stop shopping where a breach occurs
- The cost of a fraudulent data breach can range from \$182 to \$350 per data record.
- Non-Compliance may be illegal in states where you are operating
 - MN first to pass PCI Compliance as law;
 - requires any company in Minnesota that suffers a data breach and is shown to have stored prohibited card data is liable and will have to reimburse banks for the cost of blocking the exposed cards and issuing new ones. Those processing fewer than 20K transactions per year are exempt.
 - Cannot store prohibited information such as PIN block beyond 48 hours
 - Similar proposals have appeared in the legislatures in Texas, California, Connecticut and Illinois
 - Effective in 2009 Massachusetts residents information will become more secure as the new state law takes effect
 - Requires similar protection standards as PCI does;
 - MA state law covers all residents' personal information including financial data

proactive > secure > confident



SDS
SECURE DIGITAL SOLUTIONS



Begin Achieving PCI Compliance

- Outsource the processing of credit cards
- Identify your merchant level
- Complete the appropriate Self Assessment Questionnaire (SAQ)
- Identify gaps in the environment based on the results of the SAQ
- Create a remediation plan
- Set a date for compliance!! Hint: No more than 12 months out.
 - this creates motivation for the key people involved

proactive > secure > confident



SDS
SECURE DIGITAL SOLUTIONS

Insurance as an Option to Augment Protection

- Taking measures to increase your state of security can reduce economic impact to the business
- Estimates for Cyber Insurance:
 - Fireman's sets premiums based on a business' annual sales. A 10-store restaurant chain might pay about \$300 annually for the core data-compromise coverage...The card coverage will cost anywhere from \$175 per account on sales below \$1 million to \$750 for businesses with sales above \$15 million."
- The Catch
 - Fireman's requires a business to have 12 months of PCI compliance under its belt and to document any previous data breaches

Source: Information Week: John Sawyer, **PCI Impact Brings Insurance Protection Offering**

proactive > secure > confident

Lessons From The Field

- Reduce scope
 - To reduce the effort and investment for compliance segment card holder systems from other non-cardholder systems
- Identify the key people required to make PCI Compliance a reality
 - Create a project team and meet together at least weekly
 - Manage the project just as any other client objective
- Document Data Flow
 - All systems which transmit, process or store cardholder data are in-scope for PCI compliance
- Review Policies and Standards
 - Ensure these cover PCI requirements and develop standards to implement the requirements inside of the in-scope environment
- Understand the cost of achieving and maintaining compliance
 - Initial compliance is costly however maintaining compliance does not necessarily need to be
 - Be sure not to overlook the cost to maintain compliance over the next 3-5 years; analyzed the same as any other asset prior to purchase

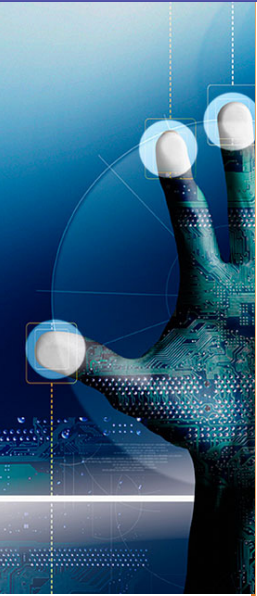
proactive > secure > confident



SDS
SECURE DIGITAL SOLUTIONS

Summary

- Determine if PCI Compliance is right for your organization; if not already mandatory.
- Identify your Merchant Level; complete the Self Assessment Questionnaire
- Establish a remediation plan and manage the plan as a key business objective
- Ensure to calculate the costs of maintaining compliance over 3-5 years
- Reduce the cost and effort of compliance by reducing the scope when and where possible





Thank You!

- Questions?
- Chad Boeckmann, CISSP, CISA,
Secure Digital Solutions
Phone: 763-234-9422
Email: ChadB@SecureDigitalSolutions.com
Web: www.SecureDigitalSolutions.com

proactive > secure > confident