
INTEGRITY • INNOVATION • EXPERIENCE


The Effects of the PCI Mandate on Your Organization

Eric M. Wright, CPA, CITP
January 19, 2010

ewright@schneiderdowns.com
(412) 697-5328


What we will be reviewing today

- What is PCI-DSS?
- Why did this happen?
- How does this effect me?
- How do I get started?
- What are the compliance requirements?
- What is covered by the requirements?
- What are the compliance deadlines?
- What are the ramifications of not complying?
- Recommendations


 © 2010 Schneider Downs & Co., Inc.

What is PCI-DSS?

- The PCI Data Security Standard (DSS) represents a set of fundamental security requirements, industry tools and measurements that address the handling of cardholder information.
- The first thing to note, PCI compliance is not required by any federal law.
- Some states have, or are in the process of enacting, legislation, but for most organizations, this compliance requirement is strictly "voluntary."
- PCI compliance requirements originally start as multiple programs administered by individual credit card companies.

 © 2010 Schneider Downs & Co., Inc.


- In December of 2004 the PCI-SSC (Security Standards Council) was established with the goal of aligning whose individual policies and procedures into one security standard that would apply to all companies involved in credit card processing
- The consortium of credit card companies that established the council included Visa, MasterCard, American Express, JCB and Discover.



SCHNEIDER DOWNS © 2010 Schneider Downs & Co., Inc.

Changes to Compliance

Payment Card Industry - Lifecycle Process for Changes to Standards



SCHNEIDER DOWNS © 2010 Schneider Downs & Co., Inc.

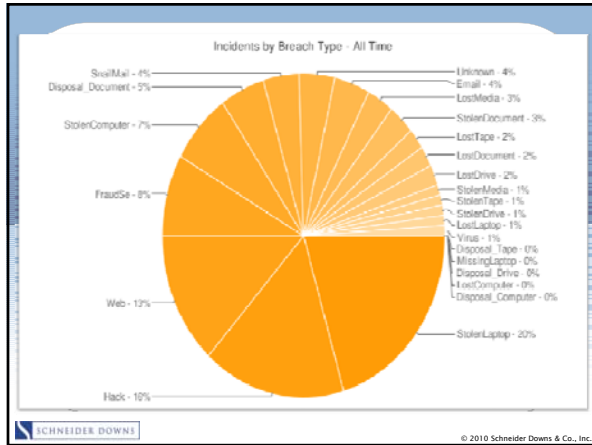
Why did this happen?

- Companies were required to comply with multiple standards based on the credit cards they accepted.
- In response to a spike in the number of data breaches over the past few years.
 - In 2009, there were 492 reported breaches affecting 222,346,827 records.
 - The selling price of single stolen record sold by thieves on the black market is \$100.
 - 15 million US residents have their identity fraudulently used every year.
 - Estimated financial losses approached \$50 billion in 2009.
 - Most common form of all identity theft is credit card fraud.

SCHNEIDER DOWNS © 2010 Schneider Downs & Co., Inc.


- **TJX Companies**
 - Eight major U.S. retailers were allegedly hacked by members of an international gang with 45.7 million payment-card records stolen (per SEC filing).
 - Once inside the companies' networks, the alleged hackers installed "sniffer" programs that would capture card numbers, as well as password and account information, as the numbers were being processed. According to a report in *The Wall Street Journal* in March 2007, the hackers left encrypted messages in the TJX systems to tell each other which files had been copied. Activity continued for 17 months.
 - TJX has said the price of the settlement deal for handling the breach would be approximately \$256 million. Industry experts believe the total cost of the breach, including legal fees, call centers and regulatory fines, will approach \$1.35 billion.
- **40% of all breaches have been made against the nonprofit sector.**

SCHNEIDER DOWNS © 2010 Schneider Downs & Co., Inc.



How does this affect me?

- Any organization, regardless of size or number of transactions, that accepts, transmits or stores any *cardholder data* is required to comply with the standards if they wish to continue accepting credit cards as a form of payment.



SCHNEIDER DOWNS © 2010 Schneider Downs & Co., Inc.

Definition of Cardholder Data

- Refers to any information contained on a customer's payment card. This includes information that is printed on either side of the card or any information contained on the magnetic strips.
- The Primary Account Number (PAN). That's the 13-16 digit number that you see on the payment card itself.
- If you store the Cardholder Name, Service Code, and/or Expiration Date in conjunction with the PAN, those items are also considered cardholder data and must be protected in the same way you would protect a PAN under PCI DSS.

SCHNEIDER DOWNS © 2010 Schneider Downs & Co., Inc.

- A truncated number, such as 123456XXXXX1234, whereby X represents MISSING data, not MASKED data, is NOT considered a PAN.
- Encrypted card data is still considered card data and falls under the compliance guidelines.

SAMPLE RECEIPT

RECEIPT FROM SCHNEIDER DOWNS

DATE: 01/15/10 RECEIPT NO: 123456789

MERCHANT: SCHNEIDER DOWNS

CARDHOLDER: J. SMITH

CARD TYPE: VISA

AMOUNT: \$100.00

TAX: \$10.00

TOTAL: \$110.00

RECEIVED BY: J. SMITH

SIGNATURE: [Signature]

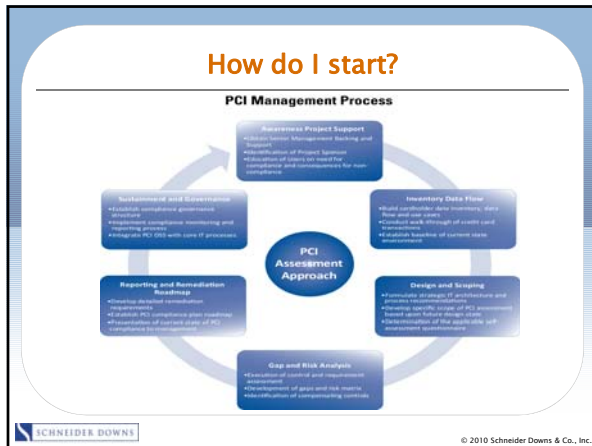
DATE: 01/15/10

SCHNEIDER DOWNS © 2010 Schneider Downs & Co., Inc.

Data you are never permitted to store

- Never store full contents of any track from the card's magnetic stripe or chip (referred to as full track, track, track 1, track 2, or magnetic stripe data).
- Never store the card-validation code (three- or four-digit number printed on the front or back of a payment card, used to validate card-not-present transactions).
- Never store the personal identification number (PIN) or PIN Block.

SCHNEIDER DOWNS © 2010 Schneider Downs & Co., Inc.



How do I start?

1. Obtain management support and build awareness.
 - Every successful project requires management's support.
 - Determine what individual(s) will be responsible for compliance.
 - Assemble a team for the various areas within your organization. This is not just an IT project.
 - Educate your staff on the need for compliance and the ramifications of not complying.
 - PCI compliance is an attitude, not a project.

© 2010 Schneider Downs & Co., Inc.

2. Inventory and document the flow of data through your system.
 - Identify where and how long cardholder data exists within your system.
 - What components of your network are involved in the processing of transactions or the storage of data.
 - Data should be classified into one of three categories:
 - Data at rest (data stored in master files)
 - Data in motion (data that resides on backup tapes)
 - Data in transmission (data transmitted over the internet)
 - Determine the volume of transactions processed annually and how those transactions are initiated.
 - Are there any third parties involved in your process?
 - Develop a flow chart documenting the processes a transaction undertakes within your organization.

© 2010 Schneider Downs & Co., Inc.

4. Complete the appropriate Self-Assessment Questionnaire

- Four questionnaires:

- **A** Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants. 13 questions that have to be addressed.
- **B** Imprint-only or stand-alone terminal merchants with no electronic cardholder data storage. 26 questions have to be addressed.



SCHNEIDER DOWNS

© 2010 Schneider Downs & Co., Inc.

- **C** Merchants with POS systems connected to the Internet, no electronic cardholder data storage. 41 questions have to be addressed.
- **D** All other merchants (not included in Types 1-3 above) 222 questions need to be addressed.

SCHNEIDER DOWNS

© 2010 Schneider Downs & Co., Inc.

Written Policies Required

Table 2
PCI DSS v1.2 Written Policy References by Self-Assessment Questionnaire Type

PCI DSS v1.2 Requirement	SAQ A (S)	SAQ B (S)	SAQ C (S)	SAQ D or ROC
3.1				
3.2				
4.2				
5.2				
6.1				
6.3.7 (a and b)				
7.1				
8.2.1				
8.3.7				
8.5.8				
9.7				
9.9				
10.10				
10.6				
10.7				
11.3				
12.1				
12.3				
12.4				
12.5				
12.6.2				
12.8 (12.8.3)				
12.9				
12.9.3				
12.9.4				
12.9.6				

SCHNEIDER DOWNS

© 2010 Schneider Downs & Co., Inc.

Requirements Addressed by the Questionnaires


Control Objective	Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3. Protect stored data. 4. Encrypt transmission of cardholder data and sensitive information across public networks.
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software. 6. Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	7. Restrict access to data by business need-to-know criteria. 8. Assign a unique ID to each person with computer access. 9. Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security.

SCHNEIDER DOWNS © 2010 Schneider Downs & Co., Inc.

5. Identify the gaps and determine if there are any compensating controls to remediate the risks.
 - Compensating controls must:
 - 1) Meet the intent and rigor of the original stated PCI DSS requirement;
 - 2) Repel a compromise attempt with similar force;
 - 3) Be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and
 - 4) Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement
 6. Address any significant gaps immediately.
 7. Complete the appropriate reports, build remediation roadmap and prepare to provide the documents upon request.
- SCHNEIDER DOWNS © 2010 Schneider Downs & Co., Inc.

Compliance Deadline


- All merchants that store, process or transmit cardholder data are supposed to be compliant now.
- Level I and II merchants' deadline of 12/31/2007 was imposed by the PCI Security Council
- The deadline enforcement for level III and IV merchants is determined by your merchant bank.
- If you have not checked with your bank, we suggest that you reach out to them, to gain an understanding of their expectations.



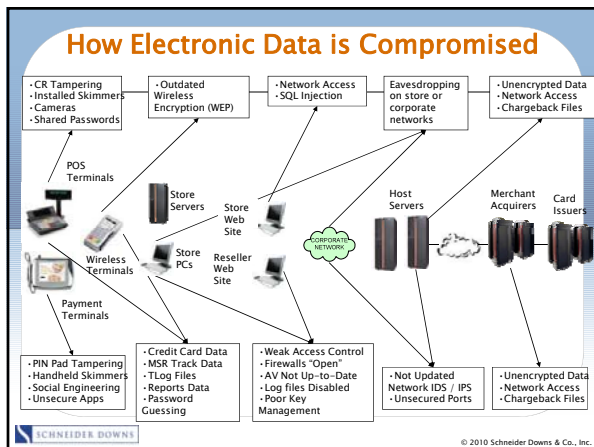
SCHNEIDER DOWNS © 2010 Schneider Downs & Co., Inc.

Ramifications of not complying

- Fines of up to \$500,000 per incident.
- Remediation cost averages \$305 per record.
- Lose the ability to process customer credit cards.
- Increase in transaction fees.
- Increase in the likelihood of legal action being taken by the cardholder whose information is stolen.
- Unwanted publicity.
- Can be fined up to \$25,000 per month until you become compliant even though data has not been breached.



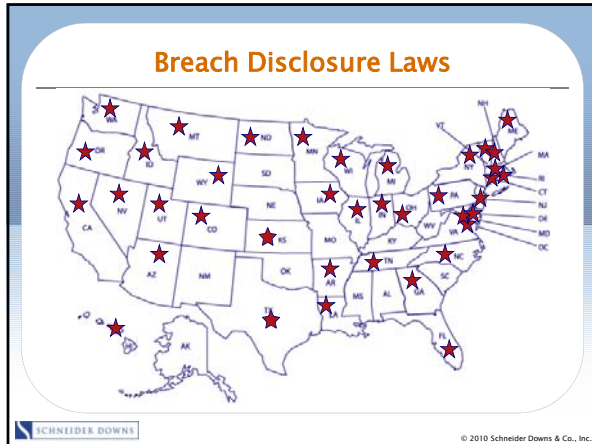
SCHNEIDER DOWNS © 2010 Schneider Downs & Co., Inc.



Other Considerations

- **Sustainability** is critical in maintaining a successful PCI-DSS compliance program.
- Need to consider manual processes and records as well as those that are processed electronically.
- Majority of breaches occur at small businesses.
- If an organization is compliant at the time of the breach, the fines are waved.
- More than 30 states have legislation in place that requires the breached organization to contact those affected by the breach.

SCHNEIDER DOWNS © 2010 Schneider Downs & Co., Inc.

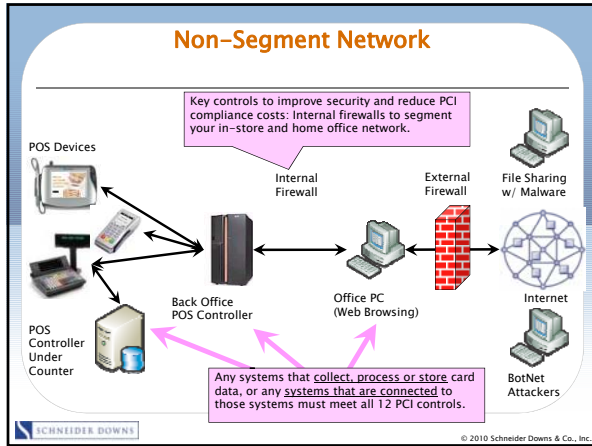


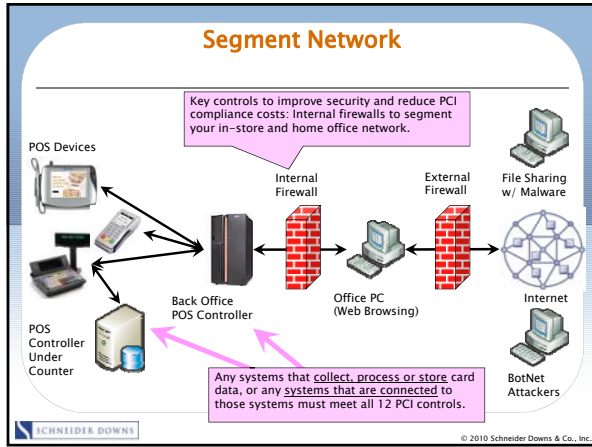
- Many states require that the compromised receive free credit protection services paid for by the organization that was breached.
- Once a merchant has suffered a hack or an attack resulting in account data being compromised, they are automatically required to meet Level 1 compliance requirements.
- Average cost of hiring a QSA on an annual basis to perform the attest function is \$50,000 – \$60,000.
- Average annual cost of hiring a ASV for quarterly scan is \$2,500.



- ### Recommendations – Start Now
1. Stop collecting card data and other confidential data you don't use.
 2. Talk to your acquirer and understand their demands & timeframes.
 3. Write / update security policies – and be sure you can meet them.
 4. Turn on monitoring functions and fix any performance impacts.
 5. Ensure individual data access is tracked via ID management system.
 6. Implement a monthly risk and vulnerability review process.
 7. Extend PCI controls to SSNs and other confidential data.
 8. Implement tools to monitor PCI compliance by service providers.
 9. Plan to replace all compensating controls over the next 1–2 years.
 - 10.Reduce PCI scope via network segmentation and data purging.







Questions?

© 2010 Schneider Downs & Co., Inc.

For Your Information

To download a copy of this presentation, please visit www.schneiderdowns.com/pci

SCHNEIDER DOWNS © 2010 Schneider Downs & Co., Inc.
