



PCI DSS Regulatory Scope Secure vs. Compliant

September 24th, 2009

Christopher Melson - CEO

Tracy Libertino-Fegarsky - VP, Professional Services

vendorsafe.com

AGENDA

- Who is Vendor Safe Technologies(VST)?
- VST Areas of Competency by PCI Control Areas
- Breach Statistics
- Industry Reality
- PCI Enforcement
- Mitigation Solutions
 - Outsourcing
 - Tokenization
 - End to End Encryption
- Holistic Approach
- PCI Security Gaps

Who is VST?

➤ Guiding Principles

- Security First and PCI will Follow
 - Network Security Specialists for 20 Years
- Lowest Cost of Ownership
 - Focused on a price sensitive market
 - Plug-and-Play technology is barrier to entry
- Scalability
 - Processes designed to deploy 2000 Firewalls /month
- Virtual Division of our customers
 - Embrace our Customer's Issues as our own



VST Areas of Competency

Requirement	Vendor Safe Solutions
Install and Maintain a Firewall	<ul style="list-style-type: none"> VST Global Security Mesh / Security Services
Change Default Passwords	<ul style="list-style-type: none"> VST Equipment and Remote Access is compliant Policy to assist client with LAN management
Protect Stored Data	<ul style="list-style-type: none"> Policy provided to address credit card data Optional VST Accusleuth to scan for credit card data on systems
Encrypt Credit Card Transmissions	<ul style="list-style-type: none"> VST equipment has the capability to encrypt to the highest standards (wired and wireless)
Updated Anti-Virus Software	<ul style="list-style-type: none"> Optional VST Managed Anti-Virus Service (Q4)
Develop Secure Applications	<ul style="list-style-type: none"> VST Does Not Manage Software Development
Restrict Access to Data	<ul style="list-style-type: none"> Hierarchical remote access VPN architecture Customer policies and procedures
Assign a unique ID for users	<ul style="list-style-type: none"> 2 factor remote access (different account for each user) Customer policies and procedures
Restrict Physical Access	<ul style="list-style-type: none"> Training material (Web Videos and Policies)
Track and Monitor Data Access	<ul style="list-style-type: none"> Optional VST Logging client available (Q4)
Regularly Test Vulnerabilities	<ul style="list-style-type: none"> Optional VST Compliance Manager
Maintain Policy and Procedures	<ul style="list-style-type: none"> VST Template Provided and maintained by customer or reseller VST available for professional services if needed

➤ Identity Theft Costs

- 51B consumers, merchants & financial institutions annually

Javelin Strategy & Research Report 2008

- PCI DSS is a “minimal foundation” for compliance
 - No Compromised entity to date has been in full compliance
 - Forensic Investigators cited that non-compliant areas were major contributors to breaches.

Adrian Phillips, Deputy Chief Risk Officer, Visa 03/16/09

Industry Reality

- Below 10% of all level 4 Merchants believe compliant (*Digital Transactions December 2008*)
- Merchants unaware of fines, higher costs and possible loss of credit card service
- Franchisees Sm. Operator / Owners unprepared
 - IT Staff non-existent
 - Small IT Staff unable to keep up with Security Standards

Full Understanding of requirements unclear

PCI Enforcement

- PCI – Is it becoming a “get out of jail free card?”
 - Safe Harbor Laws being passed in multiple states protect compliant merchants
 - Laws also requiring Merchants to adhere in Nevada, Minnesota and Massachusetts
 - Securing the card environment should be a priority (non-compliance risks further intervention and stricter involvement by the Government)

Mitigation Solutions

➤ Purpose of PCI?

- Protect the Consumer
- Minimize Credit Card Data Breaches
- Secure the Cardholder environment

Mitigation Solutions

- Prioritization of Compliance (PCI Security Council Guidelines)
 - If you don't need it, don't store it
 - Secure the Perimeter
 - Secure all Applications
 - Monitor / Control Access to systems
 - Protect Stored Cardholder Data
 - Finalize remaining compliance efforts / ensure all twelve controls are in place

Mitigation Solutions

Source of Data Breaches: Improperly Installed and Maintained POS Systems Increase Risk of Compromise

➤ *Top 3 Reasons for POS System Vulnerabilities:*

- Remote Access Security
- Host Security
- Network Security

➤ *Best Practices to Reduce Risk of Data Breaches:*

- Documented Security Policies and Procedures (no default passwords)
- Senior Executive commitment to Risk Management
- Regularly Scheduled Scanning and Penetration Testing
- Proper Monitoring and Patch Management
- Controlled code releases (and a separate development network)
- Network Segmentation to reduce credit card data retention

Source: CISP Bulletin Visa

Mitigation Solutions

➤ Outsourcing Priorities

- Firewall / Network Management
- Secure Wireless Solutions
- Encryption / Two-Factor Authentication
- Security Patch Management
- POS Reseller (Application / Software Patching)
- Centralized Anti-Virus Management
- PCI Security Consulting / Policy Development

Mitigation Solutions

➤ Tokenization

- At first glance compelling
- Myth: Tokenization is all that is required
- Heterogeneous Restaurant Environment
 - Effective Implementation Costly
 - Payment Data Integrated w/ central Tokenization Server
 - Logistical, tactical, budgeting constraints
 - In house experts may be needed for maintenance
- Operational Policies & Controls Still Needed
- Data stored with Processor more tempting to hackers – Insurance / Hardened Contracts needed

Mitigation Solutions

➤ Tokenization

- Helps to minimize the scope of PCI
- Does not replace PCI Compliance
- Adoption increasing
- Penny's added to already "too high"
Interchange and Transaction costs
 - Average 1.7% Interchange Fees
 - Convenience Stores alone 7.6B
 - Visa increased Usage Fees in April by 2 cents per Transaction (NACS 2009)

Mitigation Solutions

- Tokenization Outsourcing (Considerations)
 - Transparency
 - Availability
 - Performance
 - Scalability
 - Security

Mitigation Solutions

- End to End (E2E)Encryption
 - Driven by Heartland
 - Solution for Recent Breach
 - Requires Centralized Management
 - Single Source Chargeback Management
 - Single Encryption
 - No more encrypt, decrypt, re-encrypt
 - Still only one area of twelve controls
 - Not Available / Slow Adoption Expected

➤ Risk Based Prioritization

- Delete Legacy Credit Card Data
- Secure Firewalls
- PA-DSS Applications
- PED Devices / PTS (Pin Transaction Security)
- Secure Remote Communications
 - (Two-Factor)
 - Individual Log on
- Monitor /Manage/Control Access to Systems
 - Network
 - Local Devices
 - Online / Wireless Activity
- Solid Operational Policies / Procedures

PCI Security Gaps

➤ Secure vs. Compliant

- Largest breaches through wireless
- Rogue Device Detection
- Intrusion Prevention / Detection not enough
- System Logging Too Expensive
- Port Lock Downs
- Wireless (Cell, Air Cards, etc)
- Security Patch Management timeliness

Patch Management

- Security / Antivirus / Compliant Applications
 - Centralized
 - Automated
 - Timely
 - Real-Time Monitoring
 - Non-Disruptive

Open Discussion

Q&A

Contact Information

For supporting documents and information contact:

- Tracy Libertino, VP -Professional Services
tlibertino@vendorsafe.com
(O) 713-929-0227 (M) 704-491-5804

URL: www.vendorsafe.com

Regulatory data source:

www.pcisecuritystandards.org