Overcoming PCI Compliance Challenges

Randy Rosenbaum - Security Services Exec. Alert Logic, CPISM
Brian Anderson - Product Manager, Security Services, SunGard AS
Goal:

- Understand the common missteps that occur for companies when addressing PCI Compliance
- Establish an understanding of the collaborative effort required for compliance

Benefits:

- Minimize risk of a breach
- Reduce the complexity to achieving compliance
- Increase speed in identifying and responding to threats
- Reduce resource costs of maintaining compliance
SUNGARD Availibility Services

- Experience: over 30 years (1978)
- Headquarters: Wayne, PA
- Employees & Staff: 3,000+
- Customers: 9,000+
- 80 Facilities in 10 countries
- Approximately 5 Million Sq Ft of data center operations space
- Broad Portfolio of Services:
  - Managed Services
  - Recovery Services
  - Consulting Services
  - Software
- Serving wide variety of industries including, retail, financial, insurance, manufacturing & transportation/communication

SUNGARD

- Founded: 2002
- Headquarters: Houston, TX
- Employees & Staff: 100+
- Customers: 1,200+
- 50+ revenue-generating partners
- 100% recurring revenue
  - January 2011 run rate: $18M
  - Churn < .75%
- 2010 GAAP Revenue: $15M
  - 42% Y/Y revenue growth
  - 55% Y/Y growth in new bookings
- EBITDA positive and growing
Overcoming the 3 Biggest PCI Challenges
Market Trends: The Facts

- 761 security breaches in 2010 (141 in 2009)
- 89% of victims subject to PCI DSS had not achieved compliance
- 86% of the breaches were discovered by a third party
- 86% of the victims had evidence of the breach in their log files
- 96% of breaches were avoidable through simple or intermediate controls

* Source: All data is from the 2011 Verizon Business Data Breach Investigation
2010 Payment Card Industry Compliance Report

Organizations struggled with requirements 1, 10, and 11

Organizations do not appear to be prioritizing their compliance efforts based on the PCI DSS Prioritized Approach published by the PCI Security Standards Council

22% of organizations were validated compliant at the time of their Report on Compliance (ROC). These tended to be year after year repeat clients

All of the top 10 threat actions leading to the compromise of payment card data are well within scope of the PCI DSS

## Market Trends: 2010 Data Breaches

<table>
<thead>
<tr>
<th>Who is breaching data?</th>
<th>How do breaches occur?</th>
</tr>
</thead>
<tbody>
<tr>
<td>92% External Sources (+22%)</td>
<td>50% Hacking (+10%)</td>
</tr>
<tr>
<td>17% Inside Sources (-31%)</td>
<td>49% Malware (+11%)</td>
</tr>
<tr>
<td>&lt;1% Business Partners (-10%)</td>
<td>29% Physical Breach (+14%)</td>
</tr>
<tr>
<td>9% Multiple Partners (-18%)</td>
<td>17% Privileged Misuse (-31%)</td>
</tr>
</tbody>
</table>

### What Commonalities Exist

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Commonality</th>
</tr>
</thead>
<tbody>
<tr>
<td>92%</td>
<td>Attacks were not highly difficult</td>
</tr>
<tr>
<td>83%</td>
<td>Breaches were the result of opportunistic attacks</td>
</tr>
<tr>
<td>96%</td>
<td>Were considered avoidable through reasonable controls</td>
</tr>
</tbody>
</table>

*Source: 2011 Verizon Business Data Breach Investigation Report*
Types of Data At Risk

Source: 2011 Global Security Report
Where Companies Fail Their PCI Audit

Source: 2011 Global Security Report
Market Trends: Industries by Percent of Breaches

*Source: 2011 Verizon Business Data Breach Investigation Report*
Types of Hacking Technique by Percent of Breaches

*Source: 2011 Verizon Business Data Breach Investigation Report*
Analysis of the Statistics

- Achieving PCI compliance is necessary but not a priority
- Organizations continue to check the compliance box but then struggle to maintain compliance
- Requirements 1, 10 and 11, which are the most expensive and resource intensive, are the most difficult for organizations to implement and maintain
- Attacks are not being detected in an acceptable timeframe
- Organizations that achieve compliance are able to protect their card holder data
- Companies will continue to fail to achieve compliance due to lack of time, budget, and technical resources
PCI is Overwhelming Because...

- Large volumes of data to review
  - Log Data
  - Intrusion Data
  - Vulnerability Data
- Integration of all the alert data is technically complex
- Companies may not have security/compliance experts in house
- Organizations are not in the compliance business
The 3 Biggest PCI Challenges

- Effective and sustainable log management
  - Requirement 10
  - Manually reviewing and managing log data

- Identifying intrusions and vulnerabilities
  - Requirements 11.2 & 11.4
  - Detecting threats without chasing false alarms
  - Quickly identifying and remediating vulnerabilities

- Maintaining firewall configurations
  - Requirement 1
  - Protecting card holder data
  - Tracking and maintaining firewall configuration changes
Challenge 1: Why Log Management is Often Ineffective

- Management doesn't "get it"
- Procedures are too flexible to enforce
- Log data is not normalized
- Too much time to resolve incidents
- Criteria for breach are unclear

Source: PCI Knowledge Base, March 2009
Log Management

- Finding the right log management solution
  - Automated collection
  - Audit ready reports
  - Alerting on suspicious activity
- User friendly forensic analysis
- Ability to collect logs from any source
- Always-on, on-demand log storage
- Configure custom correlation rules and log alerts

Why does PCI require log monitoring:
Logs are evidence of everything that happens in your network

AUTOMATED COLLECTION
AUDIT READY REPORTS
ALERTING ON SUSPICIOUS ACTIVITY
Challenge 2: Intrusion Detection & Vulnerability Assessment

- **Vulnerability Assessment**
  - Quarterly vulnerability scans should be the minimum
  - Running scans is easy; tracking down vulnerabilities is hard
  - Some companies look for the easiest way to get a “clean” scan
    - “Tweaking” network configurations
    - Removing IP addresses from scope
  - IT security teams find it difficult to explain or justify scan results to management

- **Intrusion Detection**
  - Intrusion detection is often dismissed by companies due to the reputation for false positive
  - Companies buy technology to achieve compliance – but they don’t spend money or invest time needed to effectively use the tools
  - Limited expertise in IT departments to properly take action on security incidents
Vulnerability Assessment

- Use a PCI Approved Scanning Vendor (ASV)
- When choosing a vendor look for reports that provide instructions on how to fix the vulnerability
- Ensure that you can see a centralized view of your entire network

Why does PCI require Vulnerability Assessment:

Vulnerabilities are always being exploited by hackers

RUN QUARTERLY ASV SCANS
STEP BY STEP REMEDIATION INSTRUCTIONS
SCAN INTERNAL AND EXTERNAL NETWORKS
Intrusion Detection

- Detecting the intrusion is easy...knowing what to do next is difficult
- Intrusions are becoming increasingly sophisticated
  - IT staffs must have the knowledge and expertise to identify and remediate attacks
- Intrusion Detection protects both the internal and external areas of the network

Why does PCI require IDS:

IDS enables companies to protect both the perimeter and internal areas of the network

AUTOMATE THREAT DETECTION
RESPOND QUICKLY TO INCIDENTS
PROTECT CARD HOLDER DATA
Challenge 3: Managed Firewall

- Managed firewall should be configured to effectively protect card holder data
- Best practices include monitoring the firewall for configuration changes and enable strict change control processes
- An improperly configured firewall could lead to severe security breaches and compromised card holder data
- Properly managed firewalls require significant knowledge and consistent monitoring
Managed Firewall

- Proper firewall monitoring should include
  - Configuration change notification
  - Review of firewall logs
  - Blocking known malicious code

- Complying with Requirement 1
  - Establish and maintain firewall policy
  - Ensure DMZ best practices are being maintained
  - Restrict outbound card holder data leaving the environment

Why does PCI require Managed Firewall?

Protect Card Holder Data

KEY PROTECTION OF CARD HOLDER DATA
MAINTAIN PROPER CONFIGURATION
RESTRICT TRAFFIC TO PCI NETWORK SEGMENT
The 3 Biggest PCI Challenges

- Effective and sustainable log management
  - Requirement 10
  - Manually reviewing and managing log data

- Identifying intrusions and vulnerabilities
  - Requirements 11.2 & 11.4
  - Detecting threats without chasing false alarms
  - Quickly identifying and remediating vulnerabilities

- Maintaining firewall configurations
  - Requirement 1
  - Protecting card holder data
  - Tracking and maintaining firewall configuration changes
Meeting the Challenges Head On

- Move from manual to automated log management
  - Keys to success: automated alerting, and audit ready reports
- Choose a vulnerability assessment solution that aligns with your network
  - Keys to success: centralized view and remediation knowledge
- Select an intrusion detection solution that doesn’t require costly implementation, configuration and management
  - Keys to success: Implement a solution that adapts to your network security policies and minimizes the work load of your resources
PCI & Complementary Managed Services
SunGard PCI Complementary Managed Services

- **Requirement 1:** Install and maintain a firewall configuration to protect cardholder data
  - Multi-Vendor Managed Firewall Services, strict change control processes with multi-level approval, configuration of firewall rules in alignment with customer specified requirements, backup and retention of firewall configurations, PCI compliant management tools network

- **Requirement 4:** Encrypt transmission of cardholder data across open, public networks
  - Managed Firewall & VPN Services – enable the encrypted transport of customer / cardholder data across public networks

- **Requirement 5:** Use and regularly update anti-virus software or programs
  - Managed AV Services (OS Management) inclusive of server agents on PCI constrained systems
SunGard PCI Complementary Managed Services

- Requirements 7 & 8: Restrict access to cardholder data by business need to know and Assign a unique ID to each person with computer access
  - Managed Directory & Two-Factor Authentication Services – Configuration and management of AD / LDAP access parameters in concert with customer defined user groups and policies, employment of two-factor end-user authentication

- Requirement 9: Restrict physical access to cardholder data
  - Managed Hosting Services inclusive of card-key access, secure cages, secure cabinets, facility access control policies, 24 x 7 security personnel, biometric authentication
SunGard PCI Complementary Managed Services

- Requirement 10: Track and monitor all access to network resources and cardholder data
  - Log Manager & Log Review Services to track, monitor, and retain audit trails, failed and successful access attempts, correlation of activity to users and events, protection of audit trail from modification, etc.

- Requirement 11: Regularly test security systems and processes
  - Threat Manager & Active Watch inclusive of internal and external vulnerability scanning, IDS / IPS Services, annual penetration testing (through Consulting Services)
## SunGard PCI Complementary Managed Services

<table>
<thead>
<tr>
<th>PCI Requirement</th>
<th>Service(s) / Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: Install and maintain a firewall configuration to protect cardholder data</td>
<td>Managed Firewall: Formal Change Control Processes, PCI Compliant Management Network / Tools, Firewall Configuration Backup</td>
</tr>
<tr>
<td>4: Encrypt transmission of cardholder data across open, public networks</td>
<td>Managed VPN Services (SSL, IPSec), Managed Digital Certificates</td>
</tr>
<tr>
<td>5: Use and regularly update anti-virus software or programs</td>
<td>OS Management Services: Implementation / Mgmt. of server AV agents on all PCI constrained systems</td>
</tr>
<tr>
<td>7: Restrict access to cardholder data by business need to know</td>
<td>Managed Directory &amp; Two-Factor Authentication: Config. / Management of AD / LDAP parameters in concert with customer defined user groups and policies, two-factor end-user authentication</td>
</tr>
<tr>
<td>8: Assign a unique ID to each person with computer access</td>
<td>Managed Directory &amp; Two-Factor Authentication: Config. / Management of AD / LDAP parameters in concert with customer defined user groups and policies, two-factor end-user authentication</td>
</tr>
<tr>
<td>9: Restrict physical access to cardholder data</td>
<td>Managed Hosting Services: card-key access, secure cages, secure cabinets, facility access control policies, 24 x 7 security personnel, biometric authentication</td>
</tr>
<tr>
<td>10: Track and monitor all access to network resources and cardholder data</td>
<td>Log Manager &amp; Log Review: track, monitor, and retain audit trails, access attempts, correlation of activity to users and events, protection of audit trail from modification, etc.</td>
</tr>
<tr>
<td>11: Regularly test security systems and processes</td>
<td>Threat Manager &amp; Active Watch: internal and external vulnerability scanning, IDS / IPS Services, annual penetration testing</td>
</tr>
</tbody>
</table>
Questions & Answers

If you would like to direct a question to one of our presenters you can contact them at:

Brian Anderson - Brian.Anderson@sungard.com
Randy Rosenbaum- rrosenbaum@alertlogic.com

www.sungardas.com