SIGMA
AMERICA'S LEADING FUEL MARKETERS

PCI: It Never Ends. Why?

How to stay prepared?

Shekar Swamy
American Technology Corporation
St. Louis, MO

January 13, 2011

PCI Security Standards Council
PARTICIPATING ORGANIZATION

OMEGA

SIGMA
AMERICA'S LEADING FUEL MARKETERS

PCI compliance basics

- It's all about Data Security
- 12 major areas of compliance requirements – it's the minimum not the maximum
- Essentially 286 specific controls for compliance – new PCI 2.0
- Self Assessment Questionnaire (SAQ) can be daunting

OMEGA

Merchant levels

- What are the merchant levels – MasterCard or Visa
  - Level 1 – over 6 million
  - Level 2 - 1 million – 6 million
  - Level 3 – 20,000 – 1 million
  - Level 4 – Less than 20,000

SIGMA
AMERICA'S LEADING FUEL MARKETERS

Who is liable for a breach?

- At the very minimum – the entity that owns the merchant ID
- Major Oil Companies are not responsible for marketers and dealers
- Multi-store operators need to pay attention to their own compliance – and breach risk
- Don't wait for MOC to tell you what to do
- New guidelines for Franchisors and franchisees
- Liability starts at the point of breach

OMEGA

State of PCI – facts from the field

- Good security leads to compliance and keeps it that way
- 60% of breaches are external, 0ver 40% started inside
- 90% of insider breaches are deliberate malicious activity
- 94% is malware
- Backdoor – 38% of all breaches, 85% of all records
- Going after memory resident data, moments before it gets encrypted
- Malware pre-tested against 30 plus engines – created just for you!
- Remote access 34% - that's where it starts
- Please monitor your logs and create alerts based on policies
- Retailers freeze patching during busy season – hackers know this
- Most breaches go unreported
- Majority of breaches discovered through 3rd party notifications
- 86% of forensic audits – everything about the breach was in the logs

What are the fines and Who levies them?

- Visa PCI Non-compliance fines begin at $5000 per month and can be significantly higher
- A data compromise could result in further fines by Visa and MasterCard to recover monetary losses suffered by credit card issuers affected by the breach
- American Express has posted fines beginning at $50,000 for PCI Non-compliance
- A data compromise could result in Visa fines for Account Data Compromise Recovery (ADCR), which pertains to domestic issued cards
- Data Compromise Recovery Solution (DCRS), which pertains to international issued cards
- The merchant where the breach occurred is held responsible, and ADCR/ DCRS fines represent a partial recovery of those losses suffered by the issuers

What are the fines and who levies them? (cont'd)

- MasterCard fines are usually lump sum
- MasterCard levies fines for wrongful storage of magnetic stripe data and wrongful disclosure of account data
  - These fines are typically one-time fines substituted for Visa's PCI Non-compliance fines
  - MasterCard does not have a program similar to Visa's ADCR or DCRS
  - MasterCard issuers utilize the chargeback system to recoup losses resulting from fraudulent transactions and the reissuance of credit cards
  - Some issuers (e.g. Citibank) are very aggressive in pursuing monies via chargebacks while other issuers are less active

SIGMA
AMERICA'S LEADING FUEL MARKETERS

What should be your goal?

- Avoid getting breached – folks it's not worth it
- It's painful, expensive and never ending
- Get the processes in place for becoming and staying compliant

OMEGA

SIGMA
AMERICA'S LEADING FUEL MARKETERS

A Burger King Franchise chain story

- Located in Illinois and Missouri
  - 21 restaurants
  - One location breached over a year ago
  - 2 forensic audits just with Visa so far
  - 5,000 dollars per month fines levied by Visa
  - Master card just got started
  - Consuming the attention of the whole company
  - Over $150,000 spent so far
  - Now considered a Level 1 merchant – 4 years

OMEGA

SIGMA
AMERICA'S LEADING FUEL MARKETERS

How did they recover?

- Completed a detailed gap analysis performed by QSAs
- Upgraded their POS and back office systems to the latest PA-DSS compliant versions
- Implemented a system to completely monitor, log, report and maintain compliance – reviewed by QSAs
- Fines stopped after these steps were completed
- Instituted policies internally to be in compliance
- The whole company is sensitive to PCI compliance
- Now talking openly about their experience

OMEGA

SIGMA
AMERICA'S LEADING FUEL MARKETERS

PCI Compliance today

- PCI DSS moving to a 3 year cycle of changes
- PCI DSS 2.0 was released on October 28th, 2010
- Implementation started in January 2011
- If you are currently compliant with DSS 1.2 you have all of 2011 to become compliant with 2.0
- SAQ D has grown from 236 controls to 286 controls
- The council is increasing its efforts to hold acquiring banks more accountable in enforcing PCI compliance
- QSA annual reviews are getting tougher and many QSAs are on review
- Expect compliance enforcement to get a lot tougher

OMEGA

SIGMA
AMERICA'S LEADING FUEL MARKETERS

What's new in PCI ?

- Notable changes:
  - A requirement that retailers must perform extensive searches for cardholder data across all their networks and systems
  - A move to a three-year PCI lifecycle
  - Clarification on what constitutes acceptable network segmentation
  - Anti Virus and Firewall logs must be retained – 12 months
  - Wireless Intrusion Detection primarily intended for multi-site operations – unlikely to get a pass from QSAs
  - File integrity monitoring requirement is more explicit – validation of compliance
  - PA-DSS and PCI DSS becoming aligned

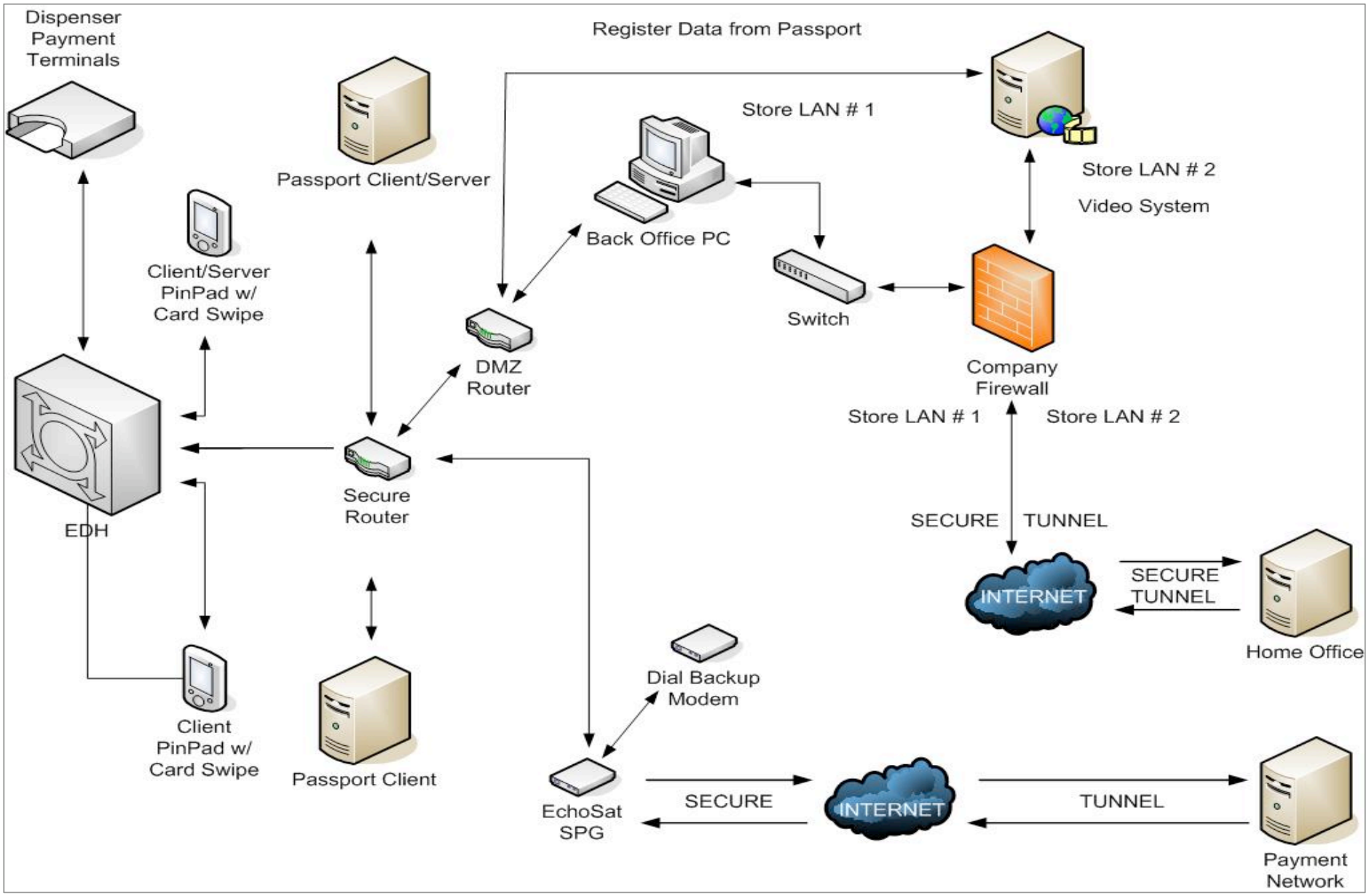
OMEGA

SIGMA
AMERICA'S LEADING FUEL MARKETERS

How to Ensure You'll Always be Compliant

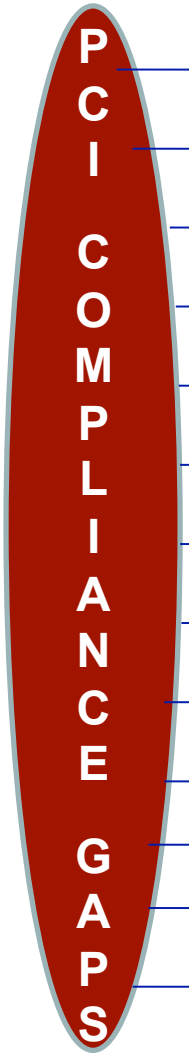
- Preparation
- Traps to Avoid
- Common Gaps
- Insider's Tips

OMEGA


Dispenser
Payment
Terminals
Register Data from Passport
Passport Client/Server
Store LAN # 1
Store LAN # 2
Video System
Back Office PC
Client/Server
PinPad w/
Card Swipe
Switch
DMZ
Router
Company
Firewall
Store LAN # 1
Store LAN # 2
EDH
Secure
Router
SECURE
TUNNEL
INTERNET
SECURE
TUNNEL
Home Office
Dial Backup
Modem
Client
PinPad w/
Card Swipe
Passport Client
EchoSat
SPG
SECURE
INTERNET
TUNNEL
Payment
Network

SIGMA
AMERICA'S LEADING FUEL MARKETERS

Common Gaps



- Unnecessary and vulnerable services not removed
- Inadequate access controls and vulnerable remote control- 2FA
- Storage of magnetic stripe data
- Lack of monitoring
- Lack of segmentation in a network
- Lack of logging - event ,firewall, and anti-virus logs
- Lack of internal system scanning
- Lack of wireless intrusion detection
- Lack of file integrity monitoring
- Lack of alerting and consolidated reporting
- Incomplete policies and procedures
- Missing and outdated security patches
- Default system settings and passwords

OMEGA

How To Ensure You'll Always Be Compliant?

- Preparation

  - ✓ Understand your service and compliance levels
  - ✓ Understand your network environment, hardware and software
  - ✓ Prepare for an audit – internally or with assistance from a service provider
  - ✓ Do a gap analysis – document it – no shortcuts
  - ✓ Determine how to address them
  - ✓ Avoid compensating controls, fix gaps right the first time
  - ✓ Find a partner to lead you through the evaluation process
  - ✓ Go through the 12 PCI DSS standards and requirements
  - ✓ Hire a Qualified Security Assessor (QSA) to Complete "Attestation of Compliance" to confirm that your business meets all PCI requirements

How To Ensure You'll Always Be Compliant? (cont'd)

- Traps to Avoid

  - ✓ Treating PCI as a technology checklist – its not a check box game
  - ✓ Focusing on the cost of PCI compliance tools
  - ✓ Not practicing PCI all year long
  - ✓ Failing to look at the whole picture
  - ✓ Getting the auditing process started too early
  - ✓ Taking systems out of scope to limit your work
  - ✓ Focus on validation of compliance - proof

How To Ensure You'll Always Be Compliant? (cont'd)

- Insider's Tips

  - ✓ Avoid manual processes for determining the state of your systems
  - ✓ Get tools and technologies in place that can assist you for a long time
  - ✓ Managed firewall service is not the entire PCI compliance process
  - ✓ Involve your senior management in discussions
  - ✓ Manage your whole environment even if systems are out of scope
  - ✓ Watch out for remote control access – first place QSAs look for problems
  - ✓ Get your act together - systems fixed and policies in place

SIGMA
AMERICA'S LEADING FUEL MARKETERS

Staying compliant requires a process

- Takes a lot of effort and requires senior management support
- Do a PCI readiness assessment
  - You can do it or have a consultant do it
  - Attempt to answer questions on SAQ
  - Take a holistic approach, nothing piece meal
- Determine the gaps
  - Start with external scanning of your sites and home office to see what are all showing up
  - Understand the extent of issues and risks

OMEGA

SIGMA
AMERICA'S LEADING FUEL MARKETERS

Staying compliant requires a process

- Find a solution to help you determine the state of your systems and fix them. Steps include:
  - External & Internal Scanning
  - Monitoring
  - Logging
  - Patching
  - Collecting data for evidence
  - Looking at the evidence to support the SAQ
- Get someone to come in and verify that you are meeting the requirements
- Continue process on an ongoing basis

OMEGA

Its like changing tires in a moving car !

Shekar Swamy

shekar.swamy@atcusa.com

Contact: 636-557-7777 x2450
Mobile: 610-639-0172