OMEGA

PCI – It Never Ends!

Shekar Swamy, President
Omega ATC

Denise Lewis, Pinnacle
POS Product Manager

PINNACLE CORPORATION

Palm POS PCI Status

- Pinnacle Palm POS is PCI compliant!
- Palm POS continues to evolve with the PCI DSS:
  - Palm passed its first PABP audit in 1997
  - All NIMs have been updated to be PA-DSS compliant
  - The first v2 PA-DSS audit will be Summer 2011
- Pinnacle PCI audits are limited to the POS environment and include Palm, Journal Manager, Pharoh and NIM
- Palm POS added security enhancements several years before PCI compliance was mandated
- Fundamental open architecture of Palm made adding PCI enhancements easier than if we used a proprietary architecture

Pinnacle and Data Security

- Pinnacle Palm POS is PCI compliant.
- Other security areas of focus besides the POS environment:
  - Remote access and support
  - QA lab
  - Privacy trends
  - Partner with security experts

About Omega and ATC

- 20 year history of performance in QSR, retail , C-store and Petroleum
- Pinnacle Partner for Data Security and Compliance
- Participating Organization in the PCI council
- Omega systems and services – widely used in the market
- NACS Data Security committee
- SIGMA sponsor and focus on PCI compliance
- 6D Data Security process

PCI DSS: It's about Data Security

- Data security is the means of ensuring that data is kept safe from corruption and access to it is suitably controlled.
- Data security helps to ensure privacy. It also helps in protecting personal data.
- It's about protecting data at your company.
- De-scoping may help you pass PCI Compliance; you are still vulnerable with Data Security.
- 12 major areas of compliance requirements – it's the minimum not the maximum, essentially 287 specific controls.

Why bother with Data Security

It's all about Protecting Your Stores – wake up!

- ✓ It’s about securing your networks and infrastructure
- ✓ It’s about securing applications and databases
- ✓ It’s about ensuring business continuity
- ✓ It’s about minimizing risk of a breach
- ✓ It’s about systems auditing and forensics
- ✓ It’s about quickly recovering from an incident
- ✓ It’s about being constantly on the vigil
- ✓ It’s about making sure that you as a merchant are in control over your destiny – not MOCs, card brands or acquiring banks
- ✓ It’s not about de-scoping
- ✓ It’s not about encrypting card numbers or filling out forms
- ✓ It’s not about just firewalls and segmentation

What should you be concerned about?

Don’t confuse filling out a form with PCI DSS - 287 controls need to be addressed

See what you will need to sign…

Part 3a. Confirmation of Compliant Status

Merchant confirms:

☐	PCI DSS Self-Assessment Questionnaire C, Version *(version of SAQ)*, was completed according to the instructions therein.
☐	All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
☐	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☐	I have read the PCI DSS and I recognize that I must maintain full PCI DSS compliance at all times.
☐	No evidence of magnetic stripe (i.e., track) data[2], CAV2, CVC2, CID, or CVV2 data[3], or PIN data[4] storage after transaction authorization was found on ANY systems reviewed during this assessment.

Part 3b. Merchant Acknowledgement

Signature of Merchant Executive Officer ↑	*Date* ↑
Merchant Executive Officer Name ↑	*Title* ↑
Merchant Company Represented ↑	

Important Areas to Pay Attention

- ✓ External scanning
- ✓ Internal scanning
- ✓ Secure encrypted remote control – 2 FA
- ✓ Patch management – regularly done and tracked
- ✓ Malware / Anti-Virus Protection – must run and keep it up-to-date – logging is required
- ✓ Network Segmentation – limits scope and reduces risk
- ✓ No cardholder data retained in the clear – you need to validate this
- ✓ Wireless intrusion detection
- ✓ Logging – the reason why this is important

Why is logging important?

- Multi-store environments where systems are remotely managed depend on proactive alerts – you need to get help
- Other logs such as system event logs patch history, application version validation, local policies, Firewall, AV, FIM are required for PCI DSS and for forensics in the event of a breach
- Centralized consolidated logs from multiple locations allows you to meet PCI DSS requirements

Why a Firewall/Router with Segmentation is not enough?

- A fully compliant solution for your business must address the controls required by PCI DSS – 287 controls
- Internal scanning
- File integrity monitoring, patching, Anti Virus
- Card data discovery
- Personal data of customers
- Real-time monitoring, anti-virus, and comprehensive logging
- 2FA-based remote control – not just remote access
- Comprehensive reporting
- May also fall short in validating – proof of compliance
- Wireless Intrusion Detection
- Who will check the checker? How will you know that your firewall is safe?

Leaving out the back office means leaving the backdoor open

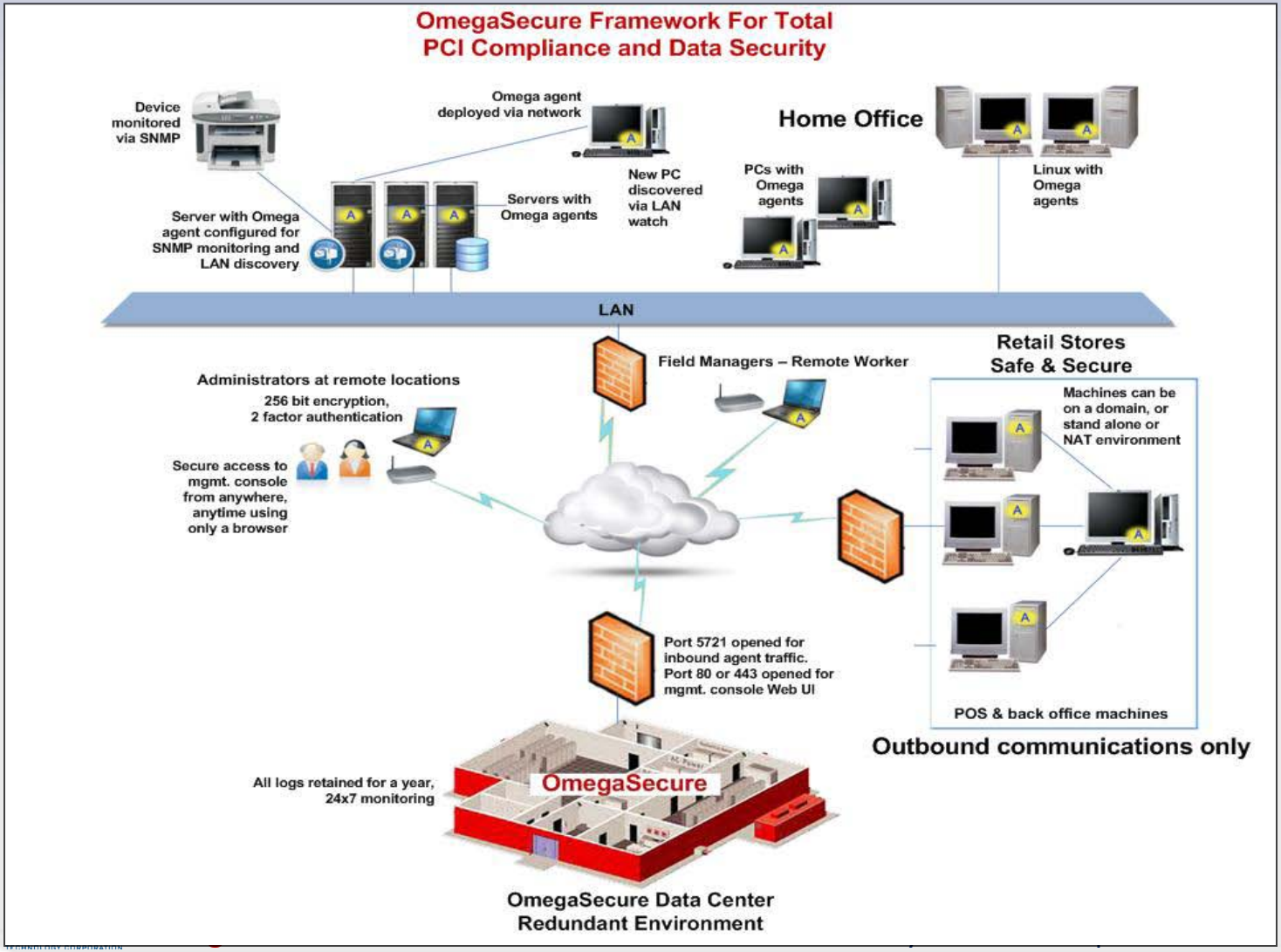
- Back office is often the entry point for remote control
- Multiple applications are housed in the same PC
- Connected to the second line
- Pulls data from POS machines
- Temporary access to the POS machines
- Contains personal information
- Home office sends data to these machines
- May have the loyalty system – personal data
- Often unprotected
- Least maintained system – patching, AV, etc not maintained

Omega Solutions

Two solutions for Data Security and Compliance

- OmegaSecure™ - A managed Service hosted at a secure data center – we do all the heavy lifting
- OmegaManager™ – system installed at the customer's data center – you manage it. Scalable and reliable
- Monitoring, remediation, logging and reporting
  - ✓ Omega addresses these areas to keep customer secure, every day – Patching, WID, POS logging, File Integrity monitoring (FIM), firewall logging, secure remote control and more
- Developing and implementing information security policies
  - ✓ Omega offers professional services to assist customers complete SAQs

Omega Data Center



- SAS 70 Type II certified
- Bank of America PCI audits
- Monitored 24/7
- Redundant architecture
- Continuous availability

Should you worry about a breach?

Heartland PAYMENT SYSTEMS®

Liberty restaurant group

BURGER KING

SONY

Recent Burger King Franchisee story

- 21 restaurants – Missouri & Illinois
  - Multiple breaches over a year ago
  - 2 forensic audits just with Visa
  - 5,000 dollars per month fines levied by Visa
  - Master Card may levy lump sum fine
  - Consumed the attention of the whole company
  - Over $250,000 spent so far (as of April 2011)
  - Now considered a Level 1 merchant – 4 years
  - Going out of business was a real possibility
  - Could not see an end to the nightmare

How did they recover?

- Upgraded their POS and back office systems to the latest PA-DSS compliant versions
- OmegaSecure and Security Strategists do all the heavy lifting to completely monitor, log, report and maintain compliance – reviewed by QSAs
- Small footprint Omega agents deployed on all systems
- Fines stopped after these steps were completed
- Instituted policies internally to be in compliance

A Developing Story
Breached on April 21, 2011

- 77 million customer records
  - Loss of personal data and card data
  - US Govt. wants to know when and how the breach was discovered, when it informed authorities and account holders
    - What steps Sony is taking to address the breach
    - Hearing on proposed data security legislation – Federal
  - Non-public personal information protection is far beyond PCI
  - Be very worried about Federal and State laws affecting customer information

What are you going to do?

- If a customer calls and says she suspects someone fraudulently used her card information at a specific store
- If there is a breach at one of your stores
- If you have to get a PCI audit done
- If the state laws require you to protect customer information

Are you going to check your SAQ C for answers?

When a breach occurs…

- QIRAs (Qualified Incident Response Assessor) don't look at SAQs – they go to PCI DSS for determination of breach
- 287 controls
- No proof – means no compliance
- Evidentiary support takes time to build
- You as a merchant will need to be prepared
- Multi-store environments are at high risk

Common Gaps

PCI COMPLIANCE GAPS

- Unnecessary and vulnerable services not removed
- Inadequate access controls and vulnerable remote control- 2FA
- Storage of magnetic stripe data
- Lack of monitoring and alerting
- 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 consolidated reporting
- Incomplete policies and procedures
- Missing and outdated security patches
- Default system settings and passwords

How To Ensure You'll Always Be Compliant?

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

plaid pantry convenience stores Case Study

- Level 2 merchant
- 103 stores
- Using Palm and Oasis
- Needed to become truly PCI compliant quickly with a team of security experts behind it
- Wanted to remain compliant
- Implemented OmegaSecure – for internal scanning logging, reporting, patching, anti-virus, remote control and updates
- All Omega agents up and running within 2 months
- No disruption to any store
- No hardware changes to any store
- Single pane secure console for access to all stores, logs, and reports

Honey Farms Case Study

- 35 locations in MA
- Using Palm and Oasis
- Were far from compliance
- No remediation, logging, secure remote control, alerting or reporting
- Implemented Omega
- Ed Freels – very data security conscious
- All systems are now secure and compliant
- Total control over all stores and processes
- Single pane of glass for all data security issues

PCI is an ongoing journey

- You cannot achieve it overnight and you are never done – applications, systems, infrastructure and policies
- No reduction in limiting the requirements to be compliant with PCI DSS – yes all 287 controls
- You still agree to be fully compliant with PCI DSS – attestation of compliance - know what you are signing
- Things change – Feds, State, Industry mandates, FTC are all intertwined
- POS vendors, network services, systems management, managed security all need to work together

Security and Compliance

- Focus on data security and PCI compliance will fall out of it
- Remediation of problems in a proactive manner is essential for data security
- Get help – there are heavy lifting requirements
- Filling out a form is not the end goal
- Single pane of glass for data security is now possible and affordable

What makes Omega remarkable?

- Omega is all about Data Security - Single pane of glass solution that is designed on the unique needs of your business
- Only solution to offer you two options - managed service or installed in-house
- Full remediation process to fix the problems that are found
- Addresses all merchant levels
- Requires no changes to your network
- With broadband or VSAT
- Security Strategists who will hold your hand
- 6D - our six step compliance process to get your to compliance
- File Integrity Monitoring - auto learning and non- intrusive
- Credit Card Data Discovery - automated with secure remediation
- True Wireless Intrusion detection

Getting Started with Omega

- Engage in a 30 minute discovery call
- 90 minute diagnostic meeting with Security Strategist
- Omega team presents detailed design
- Omega solution is delivered
- Security Strategists assist in documentation and developing policies
- Display Omega Safe & Secure™ stickers in all your stores

Questions?

PINNACLE CORPORATION

Denise Lewis
POS Product Manager
817-795-5555 X 256
dlewis@pinncorp.com
www.pinncorp.com

OMEGA

Shekar Swamy
President
636-557-7777 X 2450
Cell: 610-639-0172
shekar.swamy@omegasecure.com
www.omegasecure.com

Visit us Omega ATC at NACStech Booth # 711
Crack the code – Win $10,000