OMEGA

OmegaSecure.com

What does it mean to be secure?

Shekar Swamy, President

Omega ATC

What is Data Security?

- **Data security** is the means of ensuring that data is kept safe from corruption and access to it is suitably controlled.
- Thus **Data security** helps to ensure privacy. It also helps in protecting personal data.

Data Security

It's all about Protecting Your Stores

- ✓ 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
- ✓ Its about being constantly on the vigil
- ✓ Finally it's about making sure that you as a merchant are in control over your destiny

PCI is an ongoing journey

- You cannot achieve it overnight and you are never done – applications, systems, infrastructure and policies
- Significant accomplishment in reducing reporting requirements (SAQ C) for smaller merchants
- No reduction in limiting the requirements to be compliant with PCI DSS
- You still agree to be fully compliant with PCI DSS – attestation of compliance - know what you are signing

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 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

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

When a breach occurs…

- QIRAs (Qualified Incident Response Assessor) don't look at SAQs – they go to PCI DSS for determination of compliance and cause of breach
- 286 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

C-store employee impact on Data Security

- Your first line of defense
- Well-crafted policies followed by employees offers you the best protection
- People need to know what to look for and what to do to protect information and systems
- Employee turnover requires change management
- Incidence response plan depends on good policies

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