PCI 3.0: COMPLIANCE REQUIREMENTS, BEST PRACTICES AND PITFALLS

peer1 hosting

ALERT LOGIC

Agenda

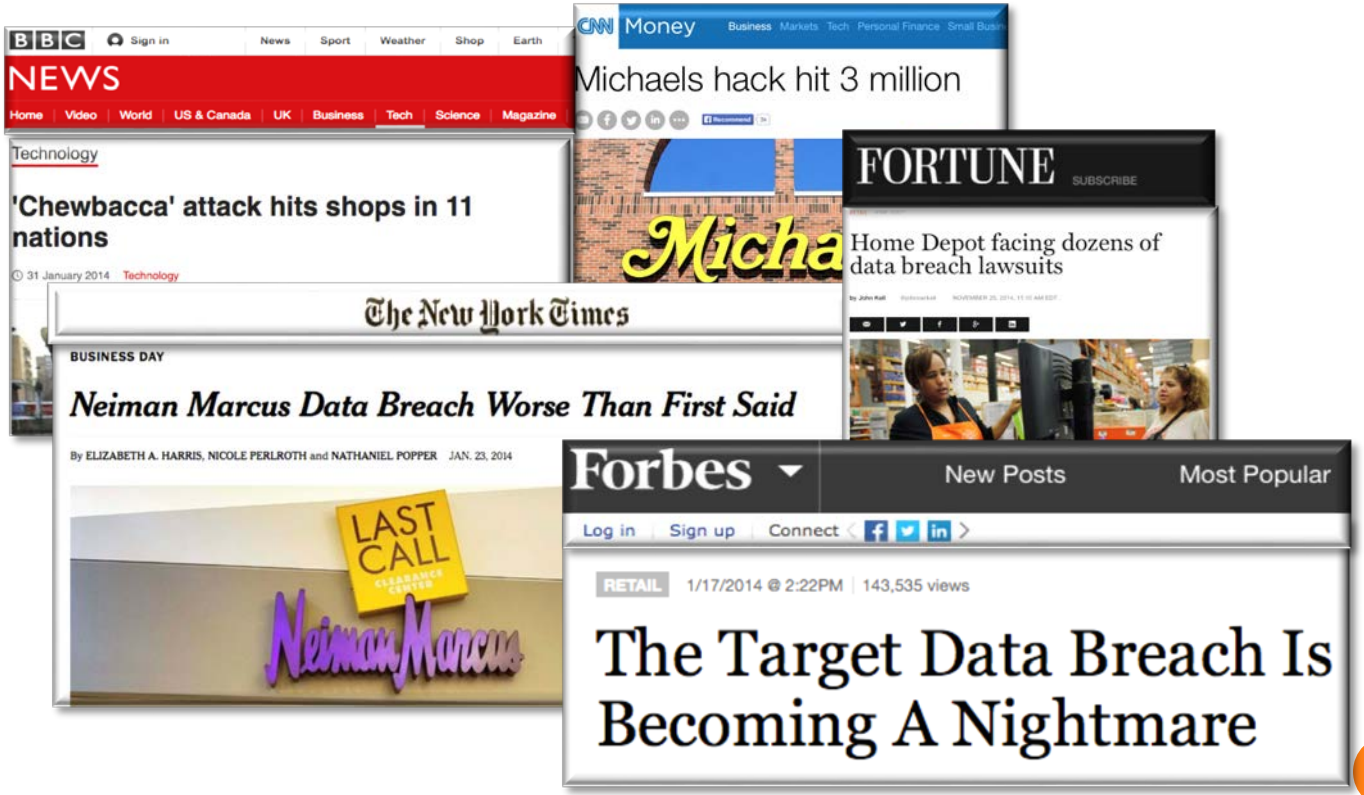
- Why is PCI Compliance important for eCommerce?
- Who needs to be PCI Compliant?
- How to achieve PCI Compliance?
- Next Steps to achieve PCI 3.0 Compliance – Technologies & Tools

WHY IS PCI COMPLIANCE IMPORTANT?

ALERT LOGIC®

The End Goal of Compliance is Security

Attacks are going to happen



ALERT LOGIC

Most Organizations are Not Fully Compliant

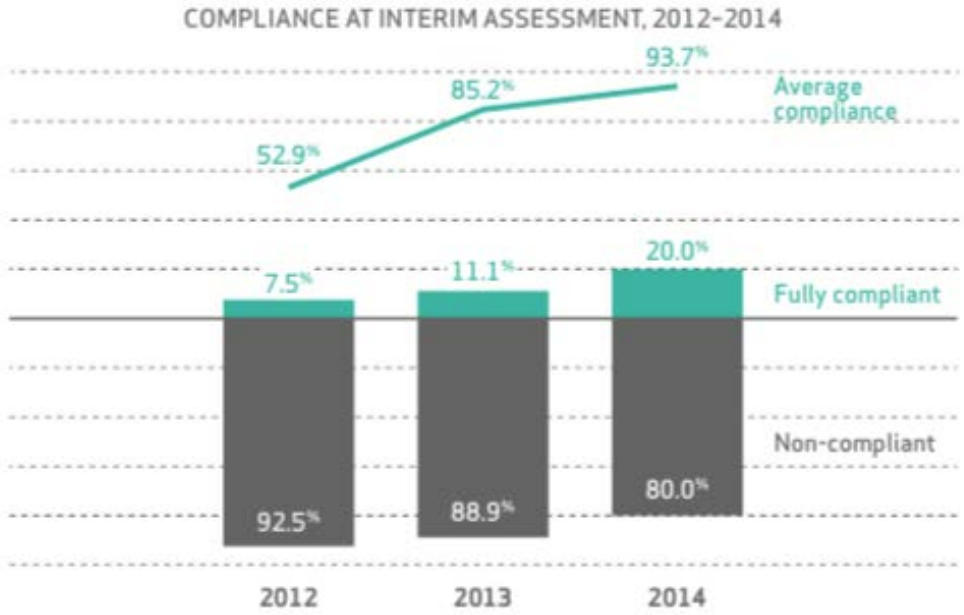


Figure 10. The overall state of PCI DSS compliance at interim assessment, 2012–2014

Source: Verizon 2015 PCI Compliance Report

WHO NEEDS TO BE COMPLIANT?

PCI DSS 3.0: More Detail, More Precision

Two Constituencies:

1. Those who have rigorous, third-party PCI DSS assessment

   = Business as Usual

2. Those who don't (SAQ, assessor who draws scope very narrowly)

   = Significant Changes

Scoping Change: Service Providers

> Parties should clearly identify the services and system components which are included in the scope of the service provider's PCI DSS assessment, the specific PCI DSS requirements covered by the service provider, and any requirements which are the responsibility of the service provider's customers to include in their own PCI DSS reviews. For example, a managed hosting provider should clearly define which of their IP addresses are scanned as part of their quarterly vulnerability scan process and which IP addresses are the customer's responsibility to include in their own quarterly scans.

- Service Provider:
  - Any entity which stores, processes, or transmits cardholder data on a merchant's behalf OR
  - Any entity which manages components such as routers, firewalls, databases, physical security, and/or servers.

- If you use a service provider(s), compliance is a shared responsibility
  - Clarify roles & responsibilities requirement by requirement
  - If relying on a service provider Report on Compliance, ensure it covers relevant requirements

Scoping Change: Continuous Compliance

To ensure security controls continue to be properly implemented, PCI DSS should be implemented into business-as-usual (BAU) activities as part of an entity's overall security strategy. This enables an entity to monitor the effectiveness of their security controls on an ongoing basis, and maintain their PCI DSS compliant environment in between PCI DSS assessments. Examples of how PCI DSS should be incorporated into BAU activities include but are not limited to:

1. Monitoring of security controls—such as firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), file-integrity monitoring (FIM), anti-virus, access controls, etc.—to ensure they are operating effectively and as intended.
2. Ensuring that all failures in security controls are detected and responded to in a timely manner. Processes to respond to security control failures should include:
   - Restoring the security control
   - Identifying the cause of failure
   - Identifying and addressing any security issues that arose during the failure of the security control
   - Implementing mitigation (such as process or technical controls) to prevent the cause of the failure recurring
   - Resuming monitoring of the security control, perhaps with enhanced monitoring for a period of time, to verify the control is operating effectively
3. Review changes to the environment (for example, addition of new systems, changes in system or network configurations) prior to completion of the change, and perform the following:
   - Determine the potential impact to PCI DSS scope (for example, a new firewall rule that permits connectivity between a system in the CDE and another system could bring additional systems or networks into scope for PCI DSS).
   - Identify PCI DSS requirements applicable to systems and networks affected by the changes (for example, if a new system is in scope for PCI DSS, it would need to be configured per system configuration standards, including FIM, AV, patches, audit logging, etc., and would need to be added to the quarterly vulnerability scan schedule).
   - Update PCI DSS scope and implement security controls as appropriate.
4. Changes to organizational structure (for example, a company merger or acquisition) should result in formal review of the impact to PCI DSS scope and requirements.
5. Periodic reviews and communications should be performed to confirm that PCI DSS requirements continue to be in place and personnel are following secure processes. These periodic reviews should cover all facilities and locations, including retail outlets, data centers, etc., and include reviewing system components (or samples of system components), to verify that PCI DSS requirements continue to be in place—for example, configuration standards have been applied, patches and AV are up to date, audit logs are being reviewed, and so on. The frequency of periodic reviews should be determined by the entity as appropriate for the size and complexity of their environment.

   These reviews can also be used to verify that appropriate evidence is being maintained—for example, audit logs, vulnerability scan reports, firewall reviews, etc.—to assist the entity's preparation for their next compliance assessment.

Continuous Compliance Implications

"...enables an entity to monitor the effectiveness of their security controls on an ongoing basis, and maintain their ... compliance ... between assessments."

- NOT a change, but a clarification
- PCI DSS has always been about continuous compliance
- Business objective should be liability mitigation, not passing an assessment
  - Breach Prevention
  - Early Detection and Containment
  - "Safe Harbor"

There are 62 Clarifications in PCI DSS 3.0

- PCI DSS 2.0 requirement ->
  Testing procedure + Navigating the PCI DSS
  - Testing procedures = Secret PCI DSS decoder ring
  - Testing procedures are more prescriptive
  - Testing procedures dictate the proper interpretation of the requirement
  - Navigating the PCI DSS provided useful guidance and clarification of intent
- PCI DSS 3.0 has reconciled requirements with testing procedure language
- PCI DSS 3.0 now includes intent column

E.g. Requirement 5.2 in PCI DSS 2.0

5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.	**5.2** Verify that all anti-virus software is current, actively running, and generating logs by performing the following:
	5.2.a Obtain and examine the policy and verify that it requires updating of anti-virus software and definitions.
	5.2.b Verify that the master installation of the software is enabled for automatic updates and periodic scans.
	5.2.c For a sample of system components including all operating system types commonly affected by malicious software, verify that automatic updates and periodic scans are enabled.
	5.2.d For a sample of system components, verify that anti-virus software log generation is enabled and that such logs are retained in accordance with PCI DSS Requirement 10.7.

Navigating the PCI DSS

The best anti-virus software is limited in effectiveness if it does not have current anti-virus signatures or if it isn't active in the network or on an individual's computer.

Audit logs provide the ability to monitor virus activity and anti-virus reactions. Thus, it is imperative that anti-virus software be configured to generate audit logs and that these logs be managed in accordance with Requirement 10.

E.g. Requirement 5.2 in PCI DSS 3.0

5.2 Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current, • Perform periodic scans • Generate audit logs which are retained per PCI DSS Requirement 10.7.	**5.2.a** Examine policies and procedures to verify that anti-virus software and definitions are required to be kept up to date.	Even the best anti-virus solutions are limited in effectiveness if they are not maintained and kept current with the latest security updates, signature files, or malware protections. Audit logs provide the ability to monitor virus and malware activity and anti-malware reactions. Thus, it is imperative that anti-malware solutions be configured to generate audit logs and that these logs be managed in accordance with Requirement 10.
	5.2.b Examine anti-virus configurations, including the master installation of the software to verify anti-virus mechanisms are: • Configured to perform automatic updates, and • Configured to perform periodic scans.	
	5.2.c Examine a sample of system components, including all operating system types commonly affected by malicious software, to verify that: • The anti-virus software and definitions are current. • Periodic scans are performed.	
	5.2.d Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that: • Anti-virus software log generation is enabled, and • Logs are retained in accordance with PCI DSS Requirement 10.7.	

ALERT LOGIC

HOW TO ACHIEVE COMPLIANCE: PREPARING YOUR ORGANIZATION

ALERT LOGIC®

Preparation Checklist

1. Produce and validate a full listing of components within the CDE
2. Produce/update cardholder data flow diagrams
3. Perform (or have performed) a DSS 3.0 gap analysis
4. Review and update penetration testing methodology and service provider contracts
5. Review the requirements under 6.6 to make sure you are meeting them fully

Ensure You Have Solid Infrastructure

1. Managed Firewalls
2. Regularly updated anti-virus software
3. Log Management and Review
4. Regularly tested security systems and process
5. Experienced Support

Who to Involve?

Within Your Organization

- All IT resources
  - Network & Systems
  - Applications & Database
  - Development
- Non-IT
  - HR & Legal
  - Accounting & Finance
  - Customer Service & Training
  - Exec Team

Use External Resources

- To guide your internal resources
- All security reviews
- Penetration testing
- Secure code reviews

PCI-DSS vs PA-DSS

PCI-DSS
Payment Card Industry Data Security Standard

- Covers the environment a payment application is implemented
- Responsibility of the entity that operates environment
- All organizations that handle credit cards need to comply with PCI DSS

PA-DSS
Payment Application Data Security Standard

- Covers payment application and has necessary controls to allow for a PCI DSS compliant implementation
- Must be implemented in a PCI DSS compliant environment
- Only software vendors that make and sell payment applications need to comply with PA DSS
- Required to provide PA DSS Implementation Guide to customers

Top Guidelines in Selecting a Payment Application

1. Confirm that the application is PA-DSS Certified

2. Minimize Scope of software that is required to be PA-DSS compliant
   - Example: Magento Secure Payment Bridge is PA-DSS certified, but the rest of Magento is not subject to the certification

3. Follow closely the Implementation Guide that is required to be provided by Software Vendor since it provides specific instructions to meet PCI-DSS Compliance
   - The PA-DSS Implementation Guide must provide details on how to configure the payment application to meet PCI-DSS
   - A PA – QSA must verify that the instructions are accurate and effective and when implemented into a PCI-DSS-compliant environment, should facilitate and support customers' PCI-DSS compliance

What’s next?

Next Steps

- Complete gap analysis before formal assessment
- Find your weaknesses and fail points … soon!
- Bring all Security & Compliance “skeletons” out of the closet
- Consider separate PCI Gap & PCI Assessment teams
  - *It’s not required but fresh eyes usually help*

Good Sources for More Information

- Alert Logic: https://www.alertlogic.com/solutions/compliance/pci-dss-compliance/
- PCI Security Standards Council: https://www.pcisecuritystandards.org/
- Visa Cardholder Information Security Program: http://usa.visa.com/merchants/risk_management/cisp_overview.html
- Mastercard Site Data Protection Program: http://www.mastercard.com/us/company/en/whatwedo/site_data_protection.html
- American Express Data Security Standard: https://www.americanexpress.com/in/content/merchant/support/data-security/merchant-information.html
- Discover Information Security and Compliance: http://www.discovernetwork.com/merchants/data-security/disc.html

Q&A

Thank you.

ALERT LOGIC®