

With PCI Scope is Everything

By James Barrow

Properly scoping a PCI project will help to eliminate unneeded spending; improper scoping can lead to spending that is out of control.

Compliance with the Payment Card Industry (PCI) standard can be seen as an ominous task costing large amounts of time and money, with no real return on investment. However, the scope of PCI is *only* your cardholder environment. The PCI Data Security Standard (DSS) v1.1 states that “*The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data.*”¹ Properly scoping a PCI project will help to eliminate unneeded spending; improper scoping can lead to spending that is out of control.

Limit the scope

Limiting where cardholder information is processed, stored or transmitted limits the scope of PCI compliance and accomplishes two things:

- Reduced risk because attention is focused on areas needing additional controls
- Reduced time, effort and expense during annual audits as security efforts can target delinquent areas, deploy proper controls, and reduce auditing costs.

Where is the data?

Evaluate how cardholder data flows within the organization and determine where it is critical to store, process and or transmit this information, *and eliminate it from non-critical business paths*. Look for areas where credit card information can be consolidated and/or eliminated. The DSS again states that “*Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment.*” Although this may require restructuring of the infrastructure, the end result should be a reduction in risk and ultimately a reduction in costs: if storing cardholder data on systems unnecessarily, unnecessary controls will have to be placed on those systems.

Data at rest

One of the largest areas of concern and cost with PCI scoping is in relation to how data is stored at rest. The standard states that data should be made unreadable:

PCI DSS 3.4 – Render primary account number (PAN), at minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches:

- Strong one-way hash functions (hashed indexes)
- Truncation
- Index tokens and pads (pads must be securely stored)
- Strong cryptography with associated key management processes and procedures.

Rendering the PAN unreadable is the area where proper scoping can have a major impact. Encrypting data is not a simple undertaking. However, encrypting data on multiple systems accessed by multiple applications across multiple platforms can become an almost unattainable goal. Does it make sense to have cardholder data stored in multiple locations, each requiring its own encryption scheme? Or would it make more sense to centralize the cardholder information into a single location, and have a single encryption strategy?

Make each business unit justify storage of cardholder information. If a proper business case can be made, the organization may decide that no changes are required for that functional unit. If a unit cannot justify the need for the storing cardholder data, eliminate the data. No cardholder data means a given environment it is now out-of-scope for PCI compliance, thus eliminating the need for controls or auditing for PCI compliance.

About the Author

James Barrow is the Chief Security Engineer of (BCS)², a Charlotte, North Carolina-based computer security consulting firm. James specializes in PCI and SOX compliance consulting and can be contacted at jbarrow@bcs2.us.

¹ https://www.pcisecuritystandards.org/tech/pci_dss.htm