Best Practice

PCI Shrink-to-fit

5 Ways to downsize your PCI program to save money and reduce risks

To begin downsizing your Payment Card Industry (PCI) Data Security Standards (DSS) program it is important to remember that compliance is mandatory and regulated. The Standards apply to all systems that process, store or transmit cardholder data (credit or debit) and any systems that connect to them. The rule is clear and concise and determines the fundamental scope of your compliance program. All downsizing starts and ends with this definition.

1. Discover & Document

First identify what cardholder data you have and where you have it. You can’t shrink what you have not measured. Conduct a thorough inventory of your business operations to identify cardholder data subject to security controls. Find all the locations where you keep electronic and hard copy data in your facilities and document them.

Once located, consolidate all hard-copy storage. Be thorough in your search for soft copy data. Remember to include VoIP and mail servers, MS Outlook archives, fax, scanner and copier memory cards and include backups and 3rd party connections. This combination provides the definitive map for reducing your card data environment (CDE).

2. Destroy & De-Scope

Now look closely at every location indicated on your CDE map and ask the question: Do we need to keep cardholder data here? Take your time. Question the obvious. The rule is “less is more”. If you don’t need it; delete it. If you do need it; do you need all of it? Can you sanitise the data by removing the primary account number and expiration dates so the data becomes insufficient to fraud the card? If so, then do so. This phase presents your biggest opportunity to downsize. Be ruthless!

3. Outsource & Oversight

After you have reduced your card holder data, step back and consider what services you could outsource to a service provider such as hosting, payment processing or storage. This option may reduce the commercial and operation impact of PCI on your business, but remember that it does not relieve you of your compliance obligations.

Suppliers must provide PCI compliant environments for your systems in scope and compliance requirements must be clearly stated in their service level agreements. Are they actually compliant? Don’t take their word for it, verify their compliance status.
Audit their facilities at least annually. Get copies of their policies and procedures. Ask to see copies of their testing and scanning reports as well as their actual report on compliance (RoC). If they hesitate, find yourself another supplier.

Remember, you can outsource the activity but not the liability. If they had a breach and lost your client's card data, it would be your company's name in the papers.

4. Separate & Segment

After you've documented, deleted and outsourced everything you can, your next step is to separate your network to ensure that only those user's with a "need to know" (demonstrated business reason) can access cardholder data within the CDE.

Your objective is to minimise access. This is done through the implementation of firewalls, virtual private networks (VPN) or software. As a rule, all 3rd party and wireless networks should be segmented. All remote access to the CDE requires dual authentication of the end user. Independently test any commercial solution before its implementation.

If you're using end-to-end (point-to-point) encryption as a segmentation method don't forget that the card brands publish their own configuration requirements for point of sale (PoS) devices. These must be met if you are going to achieve segmentation. If you are using bank-owned PoS devices, verify that their configuration meets PCI requirements and that compliance requirements are clearly stated in the service level agreements.

Whatever segmentation method you decide to deploy to minimise the scope of your CDE, you will still have to implement the PCI controls (but only on the now reduced CDE) and validate your compliance to your acquiring bank.

5. Tokenisation

Finally, consider using a commercial tokenisation method to downsize the scope of your PCI program. This is when card data is replaced by a "token" (surrogate value) and stored in a centralised vault. In a tokenisation solution only those systems actually processing, storing or transmitting cardholder data remain in scope and those systems processing, storing or transmitting surrogate values are removed from the scope.

Whatever you select, make sure that you test it and verify it meets your criteria. See the PCI Security Standards Council website for guidance on implementing a tokenisation solution. While it is certainly effective in reducing your overall program it is not a silver bullet.

Best Approach

The PCI DSS is a risk management framework to help your business identify, minimise and manage the risk of compromise to cardholder data. It is not a checklist and implementing it will not prevent a breach - only reduce the likelihood of one occurring.

As the objective of the PCI DSS is risk management. If you can understand this it can result in significant savings of time, resources and finances as you will only deploy controls appropriate to the level of risk you actually have.
This is by far the best and also the right approach to take.

For more information please don’t hesitate to contact us at **0800 978 8139** or send us an enquiry via our contact form.