PCI Security Standards Council

The Art of PCI Maintenance

Managing Security Throughout the Year

Paul Brennecker,
3B Data Security Ltd

The Art of PCI Maintenance

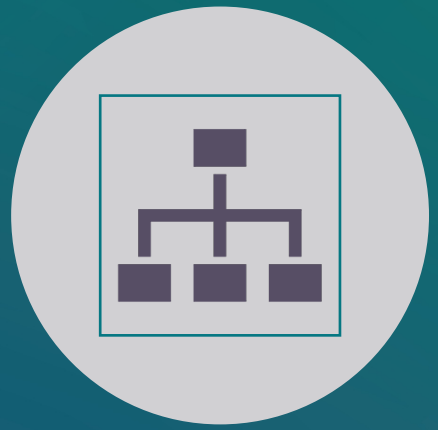
Security as a Continuous process

- A change in attitude and approach
- Maintaining a robust security posture on a 24/7/365 basis
- Move away from the “Annual Assessment” mentality
- Other benefits often come with this approach

PCI Security Standards Council

The Art of PCI Maintenance

Security as a Continuous process – Lets look at GRC



Governance;

Aligning procedures and actions with the goals of the business

Risk;

Identifying where the risks lie and how best to treat them

Compliance;

Ensuring regulatory and legal requirements are met

PCI Security Standards Council

The Art of PCI Maintenance

PCI DSS v4.0

Approaching its 20th birthday

The threat landscape is continually evolving

The global pandemic has changed habits

PCI Security Standards Council

The Art of PCI Maintenance

Evolving Controls

Analysis of the most common causes of compromise

Identifying the weakest points and areas of risk

Developing controls to help manage these risks

PCI Security Standards Council

The Art of PCI Maintenance

Taking Ownership

Anyone who has done any work with version 4.0 of the PCI DSS is now very familiar with this statement:

“Roles and responsibilities for performing activities in Requirement ‘n’ are documented, assigned, and understood.”

PCI Security Standards Council

The Art of PCI Maintenance

Taking Ownership

So, what does this really mean?

- The tasks that are required to be performed must form part of someone's role
- It could even be one of their key duties, and monitored as such
- As QSAs, we often hear interviewees say

"Oh – that's not part of my job"

or

"Ah – That task hasn't been performed since Joe left"

PCI Security Standards Council

The Art of PCI Maintenance

Documentation changes

A procedure document is required to detail how account data is stored

This also applies if you don't store CHD – state why not

It is no longer good enough to say "I don't store card data" – you must have a policy that states this and a method for checking that this is managed correctly.

PCI Security Standards Council

The Art of PCI Maintenance

Documentation changes

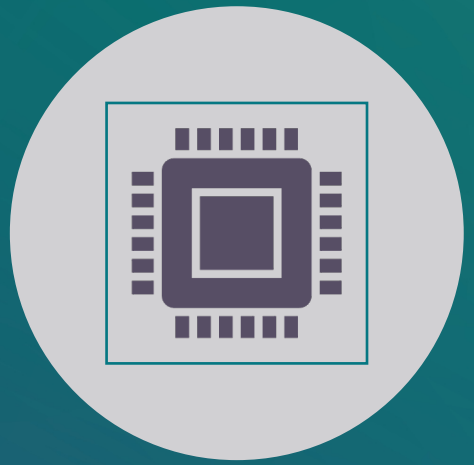
In Addition, you must have:

- Specific retention requirements – Define how long you keep data and why!
- A process for securely deleting card data when it is not required
- A process to check this is managed correctly, (at least every 3 months)

PCI Security Standards Council

The Art of PCI Maintenance

Maintaining the Environment



Not keeping on top of security patching was high on the list of problems experienced by compromised entities

This had to change as the majority of cases investigated were down to poor practise

PCI Security Standards Council

The Art of PCI Maintenance

Maintaining the Environment

Critical patches must be applied within 1 month of release

Even for websites with outsourced ecommerce payment solutions (SAQ A)

Often the status of underlying application of operating systems is not monitored

A process for checking and patching web servers is now a requirement for all eCommerce merchants

PCI Security Standards Council

The Art of PCI Maintenance

Know your Scripts!

This is a significant change, driven by analysing compromise cases

Identify which scripts are running during the checkout process

Ensure they are all valid and authorised.

PCI Security Standards Council

The Art of PCI Maintenance

Know your Scripts!

So……what do we have to look out for?

- Inventory of all the scripts that are running at the point of checkout
- These scripts must be authorised
- The Integrity of each script must also be monitored (alerting changes)
- Each script must have a business justification

PCI Security Standards Council

The Art of PCI Maintenance

Vulnerability Management

SAQ A now requires ASV scans to be run, at least quarterly

This will need to be done by an Approved Scan Vendor (ASV)

All vulnerabilities identified as ‘critical’ will need to be remediated within 30 days.

PCI Security Standards Council

The Art of PCI Maintenance

Change Detection

A change detection mechanism must be deployed when using an iFrame to connect to a PSP.

Ensuring that the code used to present the payment iframe is not subverted in some way.

Compromised entities have seen extra steps written around the iframe process.

PCI Security Standards Council

The Art of PCI Maintenance

Third Party Management

The rules around managing Third Party Suppliers have been revised

If a third party is used for processing payment card data, are they PCI compliant? How?

Using a ‘Responsibility Matrix’ to document who manages each requirement is sensible

– managed by the merchant or by the third party (s) or shared between the two.

No requirement should ‘fall through the cracks’

PCI Security Standards Council

The Art of PCI Maintenance

Third Party Management

The key rule to managing this throughout the year is –

"You can outsource anything and everything…..

…..apart from the responsibility to manage things properly!"

PCI Security Standards Council

The Art of PCI Maintenance

Summary

Many of the changes are a result of real life incidents and PFI cases!

They are all a great step forward for Ecom merchants

These controls need management throughout the year

PCI Security Standards Council

The Art of PCI Maintenance

Thank you

Paul Brennecker QSA

Head of Professional Services

3B Data Security Ltd

PCI Security Standards Council