NNT™
WORKPLACE SOLUTIONS

White Paper:

PCI DSS 3

New Standard but Same Problems?

NNT™
WORKPLACE SOLUTIONS

CHANGE TRACKER™
ENTERPRISE

Introduction

> “Cardholder data continues to be a target for criminals. Lack of education and awareness around payment security and poor implementation and maintenance of the PCI Standards leads to many of the security breaches happening today”
> *PCI SSC ‘PCI DSS 3.0 Change Highlights’ – August 2013*

Card data theft is still happening so the third revision of the PCI Data Security Standard is as much a re-launch as a revamp.

Many organizations – even Level 1 Merchants – have yet to fully implement all requirements of the PCI DSS V2 or previous versions of the standard, so eyes may well be rolling at a new version of a standard which hasn’t yet been mastered in its previous forms.

This new version is more about refinement and clarification than any introduction of new techniques or technologies to help protect against card data theft, but while losses through card fraud are still on the increase, it is clear that something has to change.

How large is the problem?

In terms of the losses being experienced, you can see why card brands, issuers and banks would still be desperate for better care and attention to be applied to their card numbers. $11Billion was lost last year and that amount is increasing yearly. Bearing in mind that the total value of card payment transactions now exceeds $21 Trillion annually, there is still plenty of money being made from the provision of fast guaranteed payment products. However, any initiative that reduces that $11 Billion loss is worthy of some time and attention. From the most recent Nilsson Report on card fraud:

> *“Card issuer losses occur mainly at the point of sale from counterfeit cards. Issuers bear the fraud loss if they give merchants authorization to accept the payment. Merchant and acquirer losses occur mainly on card-not-present (CNP) transactions on the Web, at a call center, or through mail order”*

PCI compliance isn’t just a card-brand problem that results in your organization having to spend time and money on, but is a way to protect your organization directly from serious risk. This isn’t simply a financial risk either: other factors such as brand protection and customer trust are also lost when a breach occurs.

PCI DSS Version 3.0 – Stick or Twist?

The new version of the PCI DSS isn't available until early next month so this is an early reveal of what is quite an extensive re-working of the standard. Most of the requirements are carried over with some tweaks and additions which will be covered later but there is also a degree of refinement in the wording throughout the standard.

The overall intention is that the standard aims to promote thinking about security of cardholder data rather than simply driving compliance with the standard. The Security Standards Council are, of course, keen that security best practices are adopted and practiced as a matter of routine rather than just as a 'once-a-year, big-push-to-keep-an-auditor-happy' event – as if anyone would do that? ☺

New items will be considered "best practices" until June 2015, after which they will become official requirements. Furthermore, any organization compliant with PCI DSS 2.0 can stick until January 2015 before adopting the new version of the DSS.

What Has Changed in PCI DSS V3?

So what are the specific changes or new requirements? There are wording changes throughout to encourage more routine focus on the PCI DSS requirements, but there are some detail changes and clarifying language that we can highlight here.

Requirement 2: Vulnerability Management and Hardening

Requirement 2 has always mandated the need to harden server, EPOS, and network device configurations, removing default settings as a minimum, but encouraging the adoption of a NIST or CIS hardening checklist. Detail changes for Version 3 make pass phrases acceptable. Pass phrases make a good alternative to long, complex passwords, being easier to manage and remember, but with equivalent security protection. Hardening, vulnerability management and configuration control is one of the NNT 'strong hands', and more detail is available on our website.

Requirement 6: Develop Secure Applications

6.5.6 – Insecure Handling of PAN and SAD in Memory

Just like with Buffer Overflow Protection and SQL Injection Attack mitigation, this is an appeal for application designers to be on their guard. This requirement is aimed specifically at defending against memory scraping malware, and to design in safety features so that CHD and Secure Authentication Data is protected.
The call is to take a step back and consider using programmatic features that prevent unauthorized applications from accessing memory (some development environments are better than others for this). What happens to CHD or SAD during a program crash? (Many attacks take the form of disruption to the application in order to make it 'cough up' or dump data). Where possible, can the application completely erase data when no longer needed?

In other words, this is partly an application development challenge (hence being a Requirement 6 item) but also a malware protection issue too. An attacker will need a Trojan or other Malware to scrape memory, so low level FIM can play a part in underwriting coded-protection. In summary, get ready for some more challenging questions from your QSA, so ask your EPoS/eCommerce app providers or in house development team now what they make of this requirement. Potentially this will also prove to be a difficult requirement for a QSA to validate.

6.5.11 – Broken Authentication and Session Management

The detail of this new requirement appears to be asking merchants to mitigate the risk involved with client-side takeovers: assume that trusted clients could become attack vectors. Client-side attacks are one of the most common ways hackers get access to data and as ever, hackers will go for the weakest link. The requirement also intends to put focus on man-in-the-middle style attacks as well.

Interestingly there is also a suggestion that merchants who use re-directed services (like Worldpay for example) may also need to examine their application session management operation for vulnerabilities.

Primarily this is an application design issue (Requirement 6 prefix is a giveaway ☺). It highlights a common 'vulnerability vs. functional' balance that is tolerated by developers because implementation can create user experiences that are compromised. For example, it is not going to improve sales from a retail web site if, when a customer leaves their shopping cart pre-checkout momentarily, they return to a "session timeout" message. OWASP knowledgebase is your go-to resource for development mitigation.

Requirement 8: Always Use Unique User IDs

8.5.1 – Unique Authentication Credentials for Service Providers

Standard security best practices within and outside of the PCI DSS are to always use unique access credentials for *EVERYTHING* so you know who is the perpetrator when something untoward takes place. It's just standard, good practice.

However the need for this to be explicitly highlighted as a requirement suggests that service providers need a reminder that this does apply to them too. Most service providers will be operating securely but they still need to take the same basic precautions and ensure they are using unique credentials (and not just 'customername+administrator as a username either!)

Requirement 9: Physical Security

9.9 – Protection of Point-of-Sale (POS) Devices from Tampering

Based on cardholder data theft statistics, card skimming and more elaborate variants thereof targeted on the POS equipment are still widespread. This is the ying to the yang of the previously covered, highly technical requirements, reminding Merchants that 'low tech' crime still works too.

Requirement 9 has always been intended to convey the message of 'don't let anyone touch any of the cardholder data processing equipment'. The Version 3 clarification here explicitly highlights protection of endpoints, leading to the conclusion that Requirement 9 has generally been interpreted as – rightly - being strongly oriented towards the 'central site' data center, but at the expense of focus on POS systems.

Requirement 11: Test Security

11.3 Develop and Implement a Methodology for Penetration Testing

This is another 'new' requirement that exists to emphasize focus on one of the standard practices that everyone already complies with, but maybe doesn't do it as well as they might. A classic case of meeting the letter, but not the spirit, of the requirement.

It appears that the market for Pen Testing has become highly commoditized with most vendors offering cost-engineered, highly-automated services. This inevitably has led to tests becoming more superficial (more 'checkbox approach to compliance') so this new requirement is a 'tug on the leash', forcing the merchant to avoid bad habits and corner-cutting.

This is something very key to the NNT methodology anyway, in that we advocate that classic Security Best Practices are operated, which in turn help to minimize the 'boom and bust' approach to vulnerability management that the PCI DSS sometimes engenders.

For example, running annual or quarterly scans, then having to drop everything for a week in order to patch and re-configure devices before repeating the process 3 months later not only makes life hard, but may also render you unsecure for months at a time. NNT works on a continuous basis to continually track changes to devices and allow you to operate more of a 'trimming' process to vulnerability management. This approach is more effective, gentler on the network and hosts, and easier on your resources too!

Requirement 12: Maintain a Security Policy

12.9 – Additional Requirement for Service Providers on Data Security

And finally, a clarification of Requirement 12 concerning the use of Cloud or Managed Security Services. The intention is to ensure that service providers properly understand and operate their PCI requirements fully. The DSS places the onus on the merchant to ensure they have a statement acknowledging this and, in turn, Merchants should be indemnified of cardholder data protection by their service provider.

Conclusion

In summary, while there are new requirements, some of which may prove to be challenging to implement and test, nothing changes in terms of intent.

Data security has to be a full-time focus, requiring high levels of operational discipline, with checks and balances to ensure security is being maintained. The PCI DSS attempts to convey this, but has always fallen victim to the need to educate, clarify and mandate security best practices. Data Security isn't an easy thing to describe or summarize, hence the DSS has ended up with 650 sub-requirements that the Merchant or Payment Processor find complex and ambiguous.

Technology can help, and the opportunity exists to implement highly automated solutions to the bulk of PCI requirements that are neither expensive, nor difficult, to implement and run.

And this new version of the DSS, with greater emphasis on making security a regular habit, is squarely in line with this. In fact, you could simplify the majority of the PCI DSS down to the following steps:

- Implement basic perimeter and endpoint security with Firewalls, IPS and Anti-Virus
- Audit Servers, Databases and Network Devices against NIST or CIS hardening checklists to eliminate vulnerabilities (use your FIM system for this)
- Once devices have been hardened, implement continuous vulnerability monitoring, with real-time malware detection (in other words, real-time File Integrity Monitoring)
- Instigate configuration change control to ensure devices remain secure at all times (FIM again), patch all systems monthly
- Underpin processes with logging and SIEM as a checks and balances audit trail, with regular pen testing and ASV vulnerability scans

Take these steps, and you'll not just be ahead of the curve for PCI DSS Version 3.0, but probably Version 4.0 too.

For more information go to http://www.newnettechnologies.com/file-integrity-monitoring.html