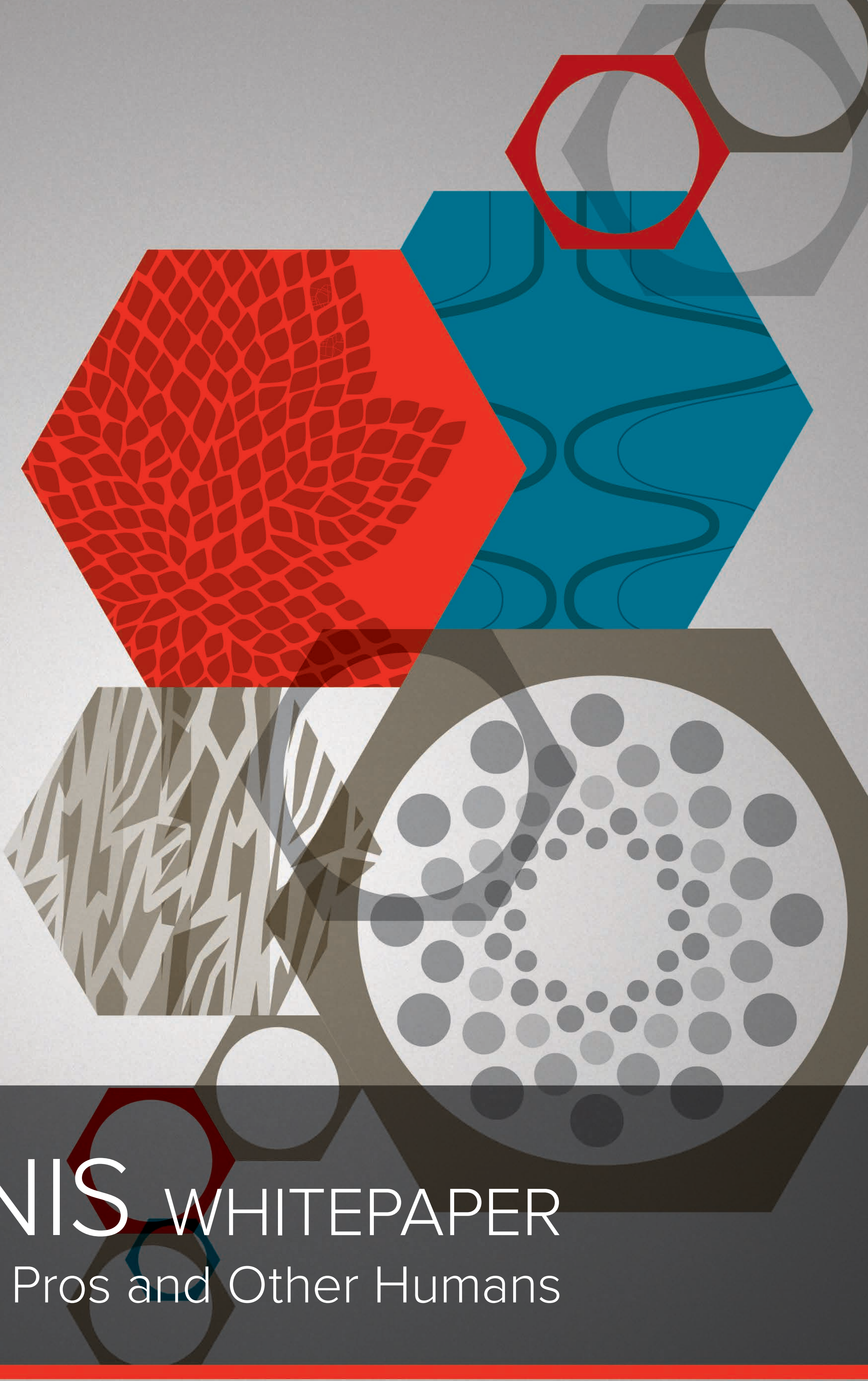


VARONIS WHITEPAPER

PCI DSS for IT Pros and Other Humans

CONTENTS

PCI DSS FOR IT PROS AND OTHER HUMANS

OVERVIEW

The Payment Card Industry Data Security Standard (PCI DSS) is not just another list of requirements for protecting data. In 2013, the number of credit and debit card transactions worldwide reached over 100 billion – that's a lot of swipes and 16-digit numbers entered.[i] PCI DSS provides the rules of the road for every small merchant, box retailer, e-commerce website, or bank that handles credit transactions.

PCI DSS is made up of almost 300 sub-requirements or controls. DSS has often been described as vague, contradictory, and difficult to fully implement. In a study conducted by Verizon, they make note of DSS's challenges:

> *There's significant variation across the individual requirements, controls, and subcontrols; as well as across industries and regions. Despite a decade of discussion, clarification, and education, there are fundamental disagreements and misunderstandings around critical areas of security and compliance…Some even regard the DSS, even in its latest 3.0 guise, as taking fundamentally the wrong approach to security*[ii]

PCI DSS may not at first appear to offer a credible model for protection against new types of hacking and more advanced malware. In the last year, major retailers who were compliant with DSS version 2.0 experienced huge data breaches wherein hackers simply went around perimeter defenses and deposited undetectable malware. In looking at this complex standard, it's easy to see how one can lose site of the forest because of all the DSS sub-control trees. In fact, PCI DSS 3.0 – released in late 2014 – now addresses new, unforeseen "real-world" threats and modern forms of attacks.

But you have to read between the lines to appreciate the full impact of PCI DSS.

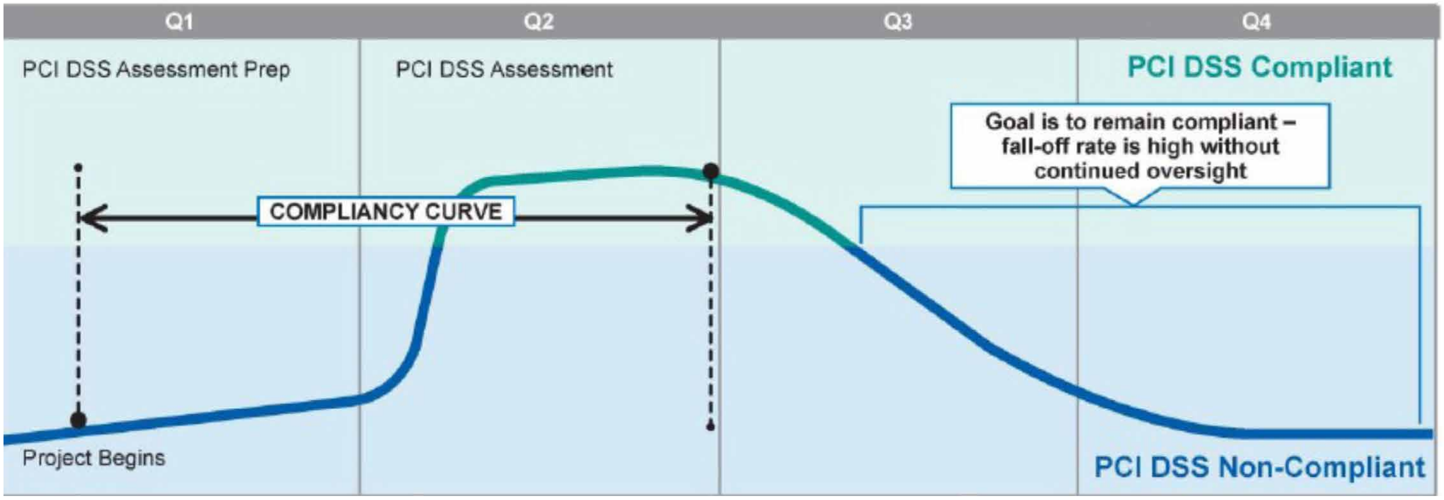
To help security practitioners, the PCI Council has provided a best practices guide for navigating the credit card security landscape. Released in 2014, Best Practices for Maintaining PCI DSS Compliance gives a high-level perspective to the 12 core security requirement. If we can summarize their best practices in a single sentence, it would go something like this: DSS is not only about meeting specific controls once a year to pass a compliance audit, but also about having programs in place for continual assessments, implementation of remediations, and monitoring.

Below, we provide a practical view of the DSS controls based on the PCI Council's own best practices advice.

PCI'S 12 STEP PROGRAM IN 3 META STEPS

In their guidance, the PCI Council emphasizes that compliance does not equate to security, and even goes as far as to say that by focusing solely on compliance, organizations may end up sacrificing security. Bottom line: DSS requirements are a pre-requisite, but not the only necessary ingredients in a data protection program.

The Council describes an all too familiar scenario: Leading up to a formal assessment conducted by a QSA, compliance and security improves as the holes and shortfalls are corrected (see graphic). After the assessment, the efforts spent on overall compliance and security drop off. To put it bluntly, organizations involved in credit card processing achieve peak security only at one point during the year.



The other issue with PCI DSS is that the requirements simply can't account for every possible security challenge. PCI DSS includes many specific granular controls, but there is also valuable data security wisdom sprinkled throughout those requirements.

For best practices, the Council suggests looking at DSS at a more abstract level. Their approach can be distilled into three intuitive ideas:

First, you need to perform a thorough risk assessment. This involves understanding potential threats, evaluating vulnerabilities, and determining what assets are at risk.

Second, you have to come up with strategies to protect IT resources, or at the very least, mitigate so that risks are reduced to an acceptable range.

Third, you need to continually monitor. You're monitoring to see whether you're compliant with the controls; you're monitoring to spot vulnerabilities (software, hardware, administrative); and you're monitoring, of course, to detect threats in progress.

We now take a closer look at these controls, and point out where DSS addresses the Council's core ideas of assessment, mitigation, and monitoring for real-world threats.

So let's take a tour through the 12 PCI DSS controls or requirements, which we've organized below into broader categories based on the above framework.

i. DATA VULNERABILITIES, HIGH RISK ASSETS, AND BASIC SECURITY MEASURES

These are the DSS controls that address both specific and general vulnerabilities, along with requiring protections for key assets – data in particular.

"Block-and-tackle" security

DSS Requirement 1

Install and maintain a firewall configuration to protect cardholder data. Firewalls are at the frontline of data security: routers are the primary means for perimeter defense. Routers can be a major vulnerability if not properly configured to block connections between untrusted parts of the network and cardholder data (1.2, 1.3).

DSS Requirement 2

Do not use vendor-supplied defaults for system passwords and other security parameters. This a very specific (and common) vulnerability that PCI explicitly calls out.

DSS Requirement 3

Protect stored cardholder data. Customer credit card data is the crown jewel. This requirement says that you should minimize the data you collect in the first place (3.1), make sure that stored data and data in-transit is unreadable (3.4, 4.1), and put in place that various cryptographic procedures (3.5).

DSS Requirement 4

Encrypt transmission of cardholder data across open, public networks. A continuation of DSS Requirement 3, but in a network setting.

DSS Requirement 9

Restrict physical access to cardholder data. Traditional brick-and-mortar security: video, key cards, etc.

Real-world software vulnerabilities

DSS Requirement 5

Protect all systems against malware and regularly update anti-virus software or programs. This is a relatively short requirement concerned with malware threats, requiring that malware and virus signatures are up to date, and that virus detection is operational.

DSS Requirement 6

Develop and maintain secure systems and applications. PCI DSS addresses both real-world software vulnerabilities (for example, injection attacks) and dispenses general advice on handling software security holes. It introduces several real-world hacker vulnerabilities: SQL and other injection attacks (6.5.1), buffer overflows (6.5.2), cross site scripting (6.5.7), insecure credential storage (6.5.3) and, significantly, insecure handling of data memory (6.5.6). It also requires procedures to be in place to find these security holes in software.

DSS Requirement 12

Maintain a policy that addresses information security for all personnel. This requirement forces organizations to have written policies in place for proper usage of cardholder data (12.1) and have assigned personnel to be responsible for responding to security alerts when there's unauthorized access (12.5).

ii. ACCESS CONTROL MITIGATIONS

Overall, DSS requires limiting access to system components through role-based access controls thereby preventing hackers from easily finding sensitive data.

DSS Requirement 7

Implement strong access control measures. Controls that limit who is authorized to access data (7.1) are an important data loss mitigation strategy.

DSS Requirement 8

Identify and authenticate access to system components. Authentication controls, particularly two-factor authentication (8.3), makes it difficult for hackers to hijack user identities – a technique used by hackers to avoid detection and move around unnoticed within the network.

iii. MONITORING

Continual testing of systems is a cornerstone in the PCI Council's guidance for DSS.

DSS Requirement 10

Track and monitor all access to network resources and cardholder data.
A series of requirements for detecting threats in progress through the monitoring of events and logs. DSS 10 forms the heart of the requirements for detection of threats by analyzing logs and audit trails (10.6).

DSS Requirement 11

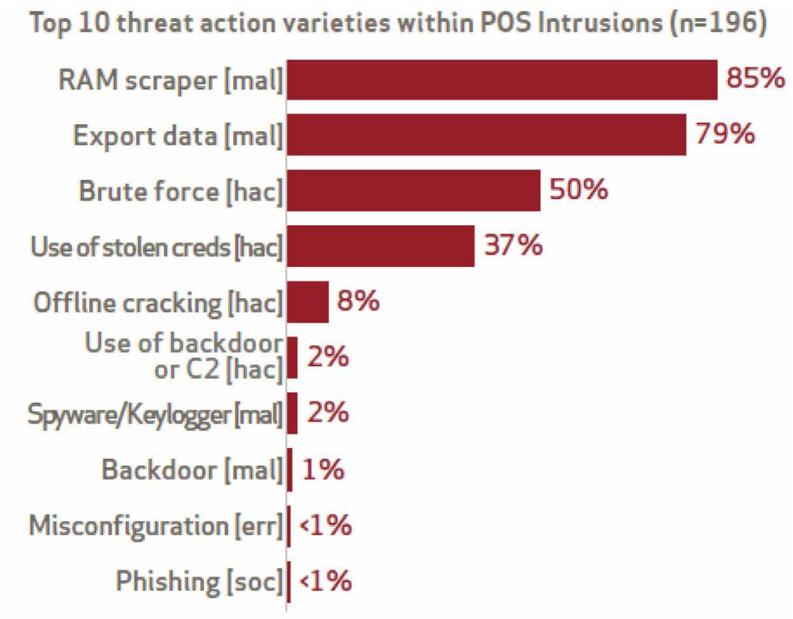
Regularly test security systems and processes. DSS 11 includes an important requirement for scanning of network ports (11.2) from an approved list of assessors. Most significantly, there's a requirement for real-world assessment by using penetration testing (11.3) to probe for vulnerabilities and find at risk data.

POINT-OF-SALE HACKING: A LOOK AT REAL-WORLD DATA

Does PCI DSS adequately address the current data security threat landscape?

To find out, let’s take a closer at the Verizon Data Breach Investigations Report (DBIR), which has been tracking the breach landscape for over 10 years.

The DBIR statistics on hacking incidents related to Point-of-Sale (PoS) are especially revealing. On the top of Verizon’s list of attack vectors and other actions are RAM scrapers, extfiltration, brute force password guessing, stolen or hacked credentials, “backdoor” exploits, and phishing.



It’s helpful at this point to now review actual PoS hacking exploits. The FBI and other analysts have worked out many (but not all) the details, and we now know that the most successful PoS-based attacks in 2013-2014 involved a depressingly familiar pattern.

To enter the retailers’ IT infrastructure, attackers likely took advantage of weak passwords and liberal lockout polices, or were able to enter through phishing and possibly SQL injection. Once inside, they moved laterally, capitalizing on of lax internal networking policies, taking on new identities by either cracking additional passwords or simply scooping up credentials through Pass the Hash.

The malware that ultimately was deposited was Backoff, BlackPos, Mozart, or its variants. These are known collectively as RAM scrapers: software that has the ability to pull out or scrape credit card data from the memory of live PoS applications. We also know that Backoff and other auxiliary malware were using explorer.exe as kind of stub to hide from IT security monitoring.

How was the credit card data ultimately removed or exfiltrated?

Based on an analysis of Backoff, Command and Control (C2) backdoor software was used to embed the HTTP data going to and from the hackers' remote site. This is another way of saying that the data was hidden in a stream of requests to web servers.

Target, Home Depot, and several other big box stores hacked in 2013-2014 were PCI compliant. This is not surprising. The major problem is that companies were passing PCI assessment tests that often fall short in adequate sampling of the infrastructure[iii]. This leads to our earlier point: security is more than just compliance.

It's easy to draw discouraging conclusions, but Verizon's security team does have some positive news. They discovered that overall companies that suffered breaches were less likely to be PCI DSS complaint.[iv]

ALWAYS BE MONITORING AND TESTING

Continuous monitoring for threats has recenlty become an important theme in security. It's not just prominent in the PCI Council's guidance for PoS, but in other standards as well. For example, the National Institute of Standards and Testing's (NIST) security framework for protecting our critical infrastructure has many controls related to continuous monitoring[v].

The importance of continuous monitoring has come about with the recognition that it may all but be impossible to prevent hackers and their malware from entering a system. Monitoring is the second-line defense that can detect and ultimately stop a hacking incident before the data has been removed or compromised.

Coupled with monitoring, IT departments should also be continually testing that their controls are working: ideally through penetration tests of their live systems. Again, it may not be possible to test all of the security holes and vulnerabilities in one sweep: it's something that must be done on an ongoing basis.

How might a continuous monitoring strategy have helped in the recent attacks on the big box retailers? We close this discussion with three actionable recommendations:

1. Monitoring can be used to check for the presence of the RAM scraper software, but has to be conducted on a granular level. In the case of BackOff and other RAM scrapers, we know that special Windows system calls are made to peek into the PoS process and pull out the credit card numbers – for example, CreateToolhelp32Snapshot and a succession of Heap32 calls are used to crawl through the heap memory. There's software available – both third-party and Windows utilities – that can monitor system call usage on the PoS server and alert IT admins when those telltale APIs are called.
2. Monitoring can spot the transfer of data files from the PoS servers to the exfiltration points. There's nothing very sophisticated going on here: BackOff malware merely launches a command shell to accomplish the data transfer. This would be an obvious red flag on a backend PoS server, and could be detected by file monitoring software.
3. Monitoring can unmask hackers who have taken over the credentials of users. The recent retail attacks have revealed how vulnerable companies are to phishing and social engineering exploits – an easy entry method for hackers. There are ways to greatly reduce the chances of intruders from stealing credentials (two-factor authentication, for example) but it may again be impossible to prevent all such incidents. However, if one has a baseline behavior of users' file access patterns – possible by collecting and analyzing file system metadata – then IT could be notified when user activity falls outside normal ranges.

While there's certainly room for improvement, the PCI DSS controls, in the context of the above framework, in fact does provides a basis for building robust security program against new threats. The key is to focus on assessment, risk reduction, and monitoring in addition to prevention.

[i] *The 2013 Federal Reserve Payment Study (frbservices.org)*

[ii] *Best Practices for Maintaining PCI DSS Compliance (pcisecuritytstandards.org)*

[iii] *Continuous Monitoring: What It Is, Why It Is Needed, and How to Use It (sans.org)*

[iv] *Verizon 2014 PCI Compliance Report (verizonenterprise.com)*

[v] *NIST Publishes Draft Implementation Guidance for Continuous Monitoring (nist.org)*

ABOUT VARONIS

Varonis is the leading provider of software solutions for unstructured, human-generated enterprise data. Varonis provides an innovative software platform that allows enterprises to map, analyze, manage and migrate their unstructured data. Varonis specializes in human-generated data, a type of unstructured data that includes an enterprise's spreadsheets, word processing documents, presentations, audio files, video files, emails, text messages and any other data created by employees. This data often contains an enterprise's financial information, product plans, strategic initiatives, intellectual property and numerous other forms of vital information. IT and business personnel deploy Varonis software for a variety of use cases, including data governance, data security, archiving, file synchronization, enhanced mobile data accessibility and information collaboration.

Free 30-day assessment:

WITHIN HOURS OF INSTALLATION

You can instantly conduct a permissions audit: File and folder access permissions and how those map to specific users and groups. You can even generate reports.

WITHIN A DAY OF INSTALLATION

Varonis DatAdvantage will begin to show you which users are accessing the data, and how.

WITHIN 3 WEEKS OF INSTALLATION

Varonis DatAdvantage will actually make highly reliable recommendations about how to limit access to files and folders to just those users who need it for their jobs.

START YOUR FREE TRIAL

WORLDWIDE HEADQUARTERS
1250 Broadway, 31st Floor, New York, NY 10001 **T** 877-292-8767 **E** sales@varonis.com **W** www.varonis.com

UNITED KINGDOM AND IRELAND
Varonis UK Ltd., Warnford Court, 29 Throgmorton Street, London, UK EC2N 2AT **T** +44 0207 947 4160 **E** sales-uk@varonis.com **W** www.varonis.com

WESTERN EUROPE
Varonis France, 13-15 rue Jean Jaures (1er Etage) 92800 Puteaux **T** +33 184 88 56 00 **E** sales-france@varonis.com **W** sites.varonis.com/fr

GERMANY, AUSTRIA AND SWITZERLAND
Varonis Deutschland GmbH, Welserstrasse 88, 90489 Nürnberg **T** +49(0) 911 8937 1111 **E** sales-germany@varonis.com **W** sites.varonis.com/de