# THE FIVE NEW PCI COMPLIANCE RULES YOU NEED TO KNOW

ENJOY SAFER TECHNOLOGY®

By Stephen Cobb, ESET senior security researcher.

If your business accepts credit or debit cards, then you know that PCI DSS stands for Payment Card Industry Data Security Standard, often referred to simply as PCI. This security standard applies to anyone who accepts, transmits, or stores any cardholder data. If your business wants to continue to do any of those things, it has to comply with PCI, the requirements of which changed significantly—from 2.0 to 3.0—at the beginning of 2015.

However, some of the new provisions were only "recommended best practices" at that point, which may have tempted some organizations to overlook them. As of July 15, 2015, they all became requirements.

Sadly, the current level of cybercrime is such that getting your business to the PCI standard is not only essential, it is the new baseline for cybersecurity as it relates to payment card data. Businesses of all sizes should strive to meet or, better yet, exceed the standards—because doing so will help improve your overall security posture.

A famous example of a company that apparently failed to meet some of the standards is Home Depot, where a 2014 breach compromised approximately 56 million of its customers' credit and debit cards. According to news reports, the company was using an outdated antimalware

solution and failed to perform regular scans on its computer systems. (PCI standards require large retailers like Home Depot to conduct such scans at least once every quarter.)

So, in case you missed them, here are five important PCI updates that you need to know about—and must now comply with—if you store, process, or transmit payment card data.

**1. Penetration Testing (PCI Compliance Requirement 11.3)**

Your systems must undergo annual penetration testing using a detailed and accepted methodology, like NIST SP 800-115. The pen test must address both the application layer (looking for issues with application logic and coding), and the network layer (configuration and maintenance of your network setup). The scope of the test includes the entire card data environment and should validate any segmentation and scope-reduction controls you have implemented.

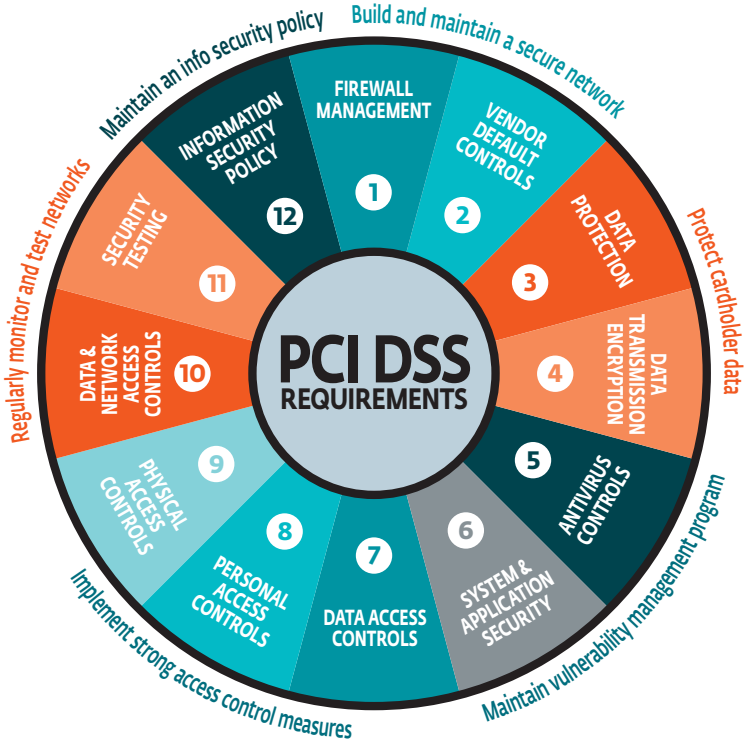
If exploitable vulnerabilities are discovered, you will need to fix them. The test process must also include "review and consideration" of any threats and vulnerabilities you have experienced in the last 12 months. And you can't just test yourself (unless you are large enough to have an in-house pen test capability that is "organizationally independent" from the people who install/maintain your systems).

If you hire an outside contractor for this aspect of your PCI compliance, and many organizations probably will, you need to make sure the contractor's testing conforms to an accepted methodology. A reputable vendor will be able to supply you with documentation of how its methodology meets this requirement, as well as appropriate professional certification of its expertise. The PCI Security Standards offers a list of approved companies and providers.

While the penetration testing requirement may seem burdensome, bear in mind that this is one of the best pieces of insurance any organization can get against data breach liability. A well-executed pen test project, through which vulnerabilities are identified and remediated, reduces the likelihood of a breach occurring and strengthens your defense if your organization is accused of neglect in the wake of a data breach.

**2. System Inventory (PCI Compliance Requirement 2.4)**

Your business must create and maintain an inventory of "system components that are in scope for PCI DSS" so as to better secure and protect them. Obviously this includes POS devices, which must be inspected periodically for tampering or substitution (you also need to train personnel to spot suspicious behavior related to devices and report tampering or swapping out).




Source: PCI DSS Requirements—alphabetacommerce.com, 2015

Not so obviously, but entirely logically, this requirement applies to all hardware (for example: virtual or physical hosts, network devices) and software (such as custom or off-the-shelf applications, internal or external) that are within the cardholder data environment. Furthermore, as Ed Moyle of ISACA has pointed out, Wi-Fi must be accounted for, per Requirement 11.1.1, which obliges you to "maintain an inventory of authorized wireless access points including a documented business justification." Note that a proper pen test will check for Wi-Fi access points in your business and verify their security settings (for example, they should all be using strong encryption, such as WPA2).

### 3. Strong Authentication (PCI Compliance Requirement 8)

If you use a third-party service provider and it has remote access to your premises, that provider has to use an authentication credential that is unique for each customer. For example, for reasons that are hopefully obvious, Joe's Card Services should not be accessing all its clients remotely with the same password. This is not something that you, as a company that accepts payment cards, has to implement. It relates to service providers, who must now go through additional examination of their authentication policies and procedures to verify that they do indeed use different authentication for servicing each customer.

What you need to do is make sure that your provider documents its compliance with this requirement to you. Note that the use of two-factor authentication with one-time codes would fulfill this requirement and is preferred by most security experts over passwords.

On the matter of passwords, there is new language in 8.2.3 which states that passwords/phrases must be at least seven characters and contain both numeric and alphabetic characters or "have complexity and strength at least equivalent" to those parameters. Frankly, those are pretty weak parameters, and it is a pity special characters are not mandated (for example, at least one of these: @#$%^&*?!).

Remember, PCI is a security baseline, and there are many situations, like this password standard, where you are free to do better and exceed the requirements.

**4. Documented Responsibility (PCI Compliance Requirement 12)**

Another requirement that affects your third-party PCI service providers concerns documenting responsibility for security. Providers must now acknowledge in writing to you that they are responsible for the security of cardholder data that they possess, store, process, or transmit on your behalf. The requirement says "to the extent that they could impact the security of the customer's cardholder data environment." This means that the parties have some latitude to negotiate where the responsibilities lie, but whatever assignment of responsibilities is agreed upon does need to be documented.

**5. Antimalware Enforcement (PCI Compliance Requirement 5)**

Your antimalware solution must now be able to manage new PCI rules that require management authorization for any disabling or altering of the operation of antivirus mechanisms. Furthermore, any disabling of the antimalware must be time-limited. In other words, your antimalware solution must be able to prevent indefinite deactivation of antimalware and ensure that antivirus mechanisms cannot be disabled or altered by unauthorized users. Note that PCI DSS 2.0 already specified that there be antivirus software in place: operational, current, and able to generate logs. What is now required is that these specifications, and secure antimalware management, be strictly enforced.

A further requirement related to malicious code concerns "evolving malware threats," which may impact systems not currently required to have antimalware. You now have a responsibility to monitor and evaluate these threats. An example would be Linux servers, which are increasingly targeted by cybercriminals but often don't have antimalware installed. These new requirements are a reminder that failure to protect these systems from malicious code could have serious consequences.

In other words, saying "we didn't know threats had evolved on those systems" will not be an acceptable excuse if a server-based malware leads to a data breach. Your goal should be to have a strong endpoint security solution with multilayered protection that covers all your networks and devices.

**Baselines and Headaches**

If some of the above sounds like a lot of work, you're not wrong, but getting that work done is not optional. While the penetration testing requirement may seem like overkill, such testing has been an IT security best practice for many years, so it is hard to argue that any system that handles sensitive data should be exempt from such tests.

Some of the changes, like keeping a close eye on your POS devices for signs of tampering and preventing people from turning off the antimalware, are just common sense. As for protecting your card data environment against evolving malicious code threats, PCI 3.0 stresses that you have a responsibility to evolve your security measures accordingly.

*Stephen Cobb has been researching information assurance and data privacy for more than 20 years, advising government agencies and some of the world's largest companies on information security strategy. Cobb also co-founded two successful IT security firms that were acquired by publicly traded companies and is the author of several books and hundreds of articles on information assurance. He has been a Certified Information System Security Professional since 1996 and is based in San Diego as part of the ESET global research team.*

*For over 25 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted. For more information, visit [www.eset.com](http://www.eset.com).*

ENJOY SAFER TECHNOLOGY®