WHITEPAPER

cavirin

CREDIT UNION PCI DSS CHALLENGES AND SOLUTIONS

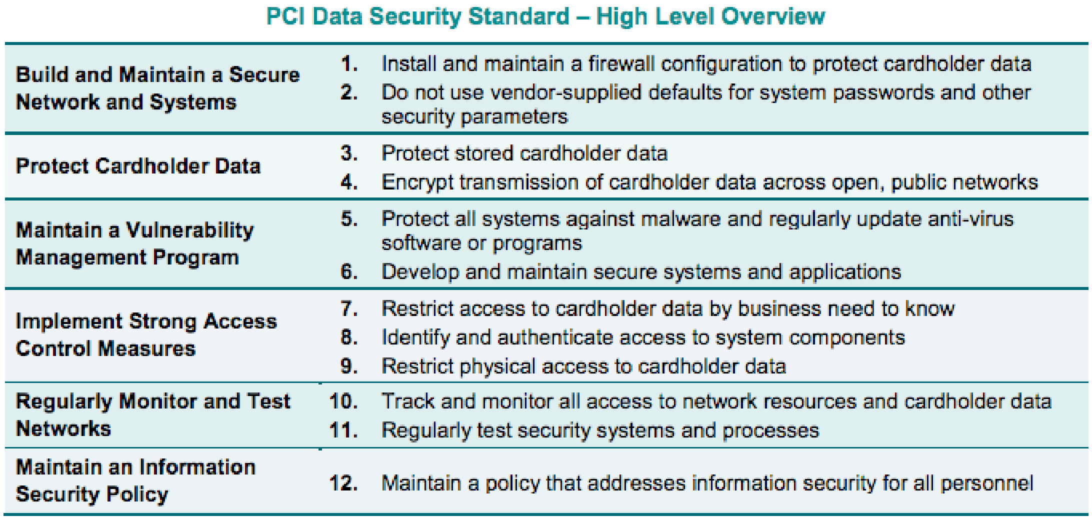
If you store, process, or transmit credit card data, you are required to meet current Payment Card Industry Data Security Standard (PCI DSS) compliances. The security standard exists to assess your company's capacity to build and maintain secure networks, protect cardholder data, sustain a vulnerability management program, implement strong access control measures, monitor and test networks, and maintain an information security policy.

If you think your company is too small to worry about PCI DSS compliance, you're wrong. There are different compliance levels, depending on your transaction volume, but every company that handles credit cards will need to meet compliance standards.

PCI DSS regulations hae become a standard in protecting credit card data. However, it is important to note that financial institutions have different protocols to follow than merchants, and for some types of institutions, like credit unions, there may be need to adopt both sets of standards. If your credit union not only issues credit cards (making it a service provider that stores members' personal information), but also accepts transactions, such as loan payments via the card or cash transactions at the teller window, the credit union acts as a merchant.

Luckily, because credit unions experience regular security audits by other compliance organizations, they already have a set of security standards in place. However, in other financial audits, they may not have to meet the same security standards as required by PCI DSS, and, therefore, may not realize they may be found in violation in a PCI audit.

There are twelve basic PCI DSS requirements that every organization handling credit card data must meet. They are:



PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

CHALLENGE

Meeting all twelve of the requirements is a challenge for any type of merchant or service provider; yet, anything under 100 percent opens the door for increased security risks, including credit card theft and compromise of cardholder personal data.

Any time a company works with a third-party vendor, it is at risk of failing to meet compliance standards. For example, a credit union may work under the belief that by outsourcing the credit card process to a third-party vendor, it is absolved from meeting PCI DSS compliance. This is a false assumption. It is the responsibility of the credit union to confirm that not only is their institution in PCI DSS compliance, but that any credit card vendor they work with is as well.

Evolving technology also adds to the complications of meeting PCI DSS compliance. Client payment information continues to sprawl across hybrid IT infrastructures including on premise, private, and public cloud platforms like Amazon Web Services and Azure. Again, outsourcing data and processes to a cloud vendor doesn't absolve you from maintaining compliance. Instead, it increases your responsibility to ensure that all of the access points to your data meets the twelve requirements.

Finally, security policies and documentation may have to cover a spectrum of regulations. If they don't include PCI's requirements, you'll need to restructure your approach.

However, even when you think that you have met all of your requirements, you may still end up failing your audit. Here are the top reasons why companies fail in compliance:

*PCI DSS requirements evolve and you might not be meeting the new requirements
*Systems get modified and aren't updated to meet PCI compliance
*Configuration standards not up to date and no longer meet PCI compliance
*You don't realize that compliance standards are necessary for data in the cloud

SOLUTION

When it's time for a PCI audit, organizations often fail for a variety of reasons, including improper security settings, incorrect configurations, low levels of encryption, or poor policies and procedures.

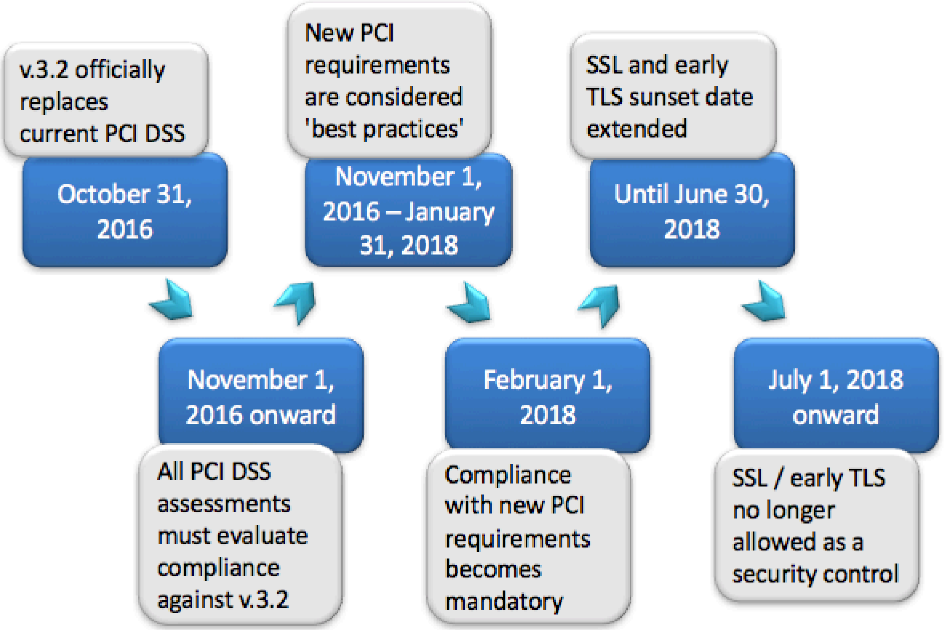
There are steps to take throughout the year to avoid possible failure (and added stress) at audit time. Adding standards controls, based on PCI DSS requirements, to day-to-day operations keeps security on the forefront and part of regular business practices. Consistently scheduled testing of security controls can help prevent added costs in business disruption as well as monetary fines, for instance. Your credit union may already be conducting such testing for other audits and regulatory institutions; if so, be sure to include the PCI requirements.

However, finding the evidence of those controls across multiple systems is sometimes impossible, especially if there is no one in-house trained to handle PCI compliance. It's why you may find the need for technology and outside professionals that can provide continuous compliance.

Carivin's continuous security assessmemnt and remediation platform offers the ability to continuously discover and monitor new devices, including the cloud, as well as any configuration changes, flagging them for potential policy violations. Cavirin is well-positioned and staffed to understand your security control requirements both in the cloud as well as on-premise and across technologies, while ensuring you will remain up-to-date in the latest compliance changes.

PCI DSS 3.2 IMPLEMENTATION TIMELINE

The clock is ticking to full PCI DSS 3.2 compliance. Major changes from v3.1 include clarification on SSL / Early TLS migration, a topic that has generated confusion. Access to any critical data now requires multi-factor authentication. Finally, there is increased scrutiny over the security practices for service providers (i.e., companies that process, store, and transmit cardholder data) that connect to merchant or institution in question.



October 31, 2016
v.3.2 officially replaces current PCI DSS

November 1, 2016 onward
All PCI DSS assessments must evaluate compliance against v.3.2

November 1, 2016 – January 31, 2018
New PCI requirements are considered 'best practices'

February 1, 2018
Compliance with new PCI requirements becomes mandatory

Until June 30, 2018
SSL and early TLS sunset date extended

July 1, 2018 onward
SSL / early TLS no longer allowed as a security control

ABOUT CAVIRIN

Cavirin provides continuous security assessment and remediation across physical, public, and hybrid clouds, supporting AWS, Microsoft Azure, Google Cloud Platform, VMware, KVM, and Docker. The company's solutions offer continuous visibility, are agentless and multi-tenant, and scale to the largest physical and virtual infrastructures. They offer up-to-the-minute compliance assessments, supplying audit-ready evidence as measured by every major regulatory and security best practice framework including CIS, DISA, PCI and HIPAA. With Cavirin, companies are empowered to make the right decisions faster and de-risk their cloud migrations.