solarwinds

SIMPLIFYING PCI COMPLIANCE FOR IT PROFESSIONALS

SOLARWINDS
WHITEPAPER

SIMPLIFYING PCI COMPLIANCE FOR IT PROFESSIONALS

If you work in just about any industry worldwide and you sell something, you likely deal with credit card processing, which involves PCI compliance. PCI is a mandatory set of requirements that applies to all credit card transactions, both physical (card present) and virtual (card not present). Even if you don't focus on PCI compliance in your daily work, every IT and security professional should be versed in the essentials of PCI. Indeed, there are many common misconceptions about PCI that can lead to costly mistakes for your organization. For example, many people believe that outsourcing credit card processing relieves you of being responsible for PCI compliance, but that is not the case. Cash fines, business reputation risk, and increased oversight are all possible outcomes from failing to properly manage a PCI program.

This paper gives you an essential overview of PCI for card-present and card-not-present transactions, as well as an update on EMV[1] card processing and how risk might shift as EMV is adopted. We'll give you some practical IT and security guidance to help you select vendors for payment processing, and determine if you can self-attest to your implementation. Finally, we include the high-level requirements for a PCI compliance credit card processing program so you can compare your current security program with PCI requirements.

A BRIEF BACKGROUND

PCI standards started in the late 1990s[2] and grew out of the need for e-commerce merchants to have a harmonized standard for security requirements, rather than the multiple, sometimes conflicting standards from VISA (CISP), American Express, JCB and others. The PCI Security Council now controls the standards that cover cyber security requirements for merchants, payment processors, financial institutions, point of sale (PoS) vendors, and hardware and software payment processing developers. Additionally, the council acts as a certifying body for vendors who wish to offer services and products to others, either for payment processing solutions or for auditing and testing.

---

[1] Originally Europay, Mastercard, Visa – this is an embedded chip technology designed to secure card present (in person) credit card transactions. Now managed by https://www.emvco.com/ which includes additional industry stakeholders.

[2] PCI timeline info graphic here: http://searchsecurity.techtarget.com/feature/The-history-of-the-PCI-DSS-standard-A-visual-timeline

CARDHOLDER DATA THREATS

Global card losses totaled $16.31 billion in 2014[3] , and there are increasingly diverse sets of bad actors that want access to cardholder data for nefarious purposes. Aside from the transactional fraud that occurs with unauthorized use (such as a friend or relative using a credit card without permission), most card fraud is motivated by either the desire to easily accumulate cash, or by ideology. Knowing the enemy, and understanding how the battlegrounds of card fraud losses are shifting (including mobile payment channels, for example), can help you advise your organization and minimize risk.

THE ENEMY

Most cyber criminals who focus on cardholder data are economically motivated. They take cardholder data and resell it on carder sites. It is such a well-known process that a search for "carder sites" brings up the hackers.freeforums.org aggregation site as a top hit. It is even possible to watch these well-known carder sites and purchase credit cards back when they show up, although no issuing bank would publically admit to using such tactics.

A less well known but more heinous motivation is the use of credit card fraud to fund terrorism. It is possible to convert fraudulently purchased airline tickets to cash, print fake credit cards, and use stolen cards to purchase tools used by terrorists, which means that an IT or security mistake can indirectly fund terrorist activities[4].

TARGETS OF OPPORTUNITY (FOR CYBER CRIMINALS)

Given the enemy's motivation, larger troves of cardholder data are generally targeted, such as the widely publicized data breaches that affected Target and Home Depot customers. But smaller businesses are also victimized, especially if they use a PoS system that has already been compromised. As early at 2007, researchers started to warn against using vulnerable PoS systems[5], yet these systems continue to be utilized.

As payments increasingly move to mobile processing, mobile has become a target of opportunity. In fact, mobile fraud measured as a percent of revenue almost doubled from 2013 to 2014 (from 0.69% of revenue to 1.36% of revenue)[6].

---

3 http://www.pymnts.com/news/2015/global-card-fraud-damages-reach-16b/

4 http://www.creditcards.com/credit-card-news/credit-cards-terrorism-1282.php

5 http://www.hackerfactor.com/papers/cc-pos-20.pdf

6 http://www.pymnts.com/news/2015/global-card-fraud-damages-reach-16b/

Since the adoption of EMV, the cards with chips that provide end-to-end encryption, card-present fraud is expected to decrease, but likely shift to card-not-present scenarios, where such fraud will likely increase. Although e-commerce still only accounts for about 10% of global retail, it is responsible for most revenue growth in retail[7]. This shift leaves plenty of room for cyber criminals to capitalize on credit card fraud, which means IT and security teams need to increase resources to protect consumers in card-not-present situations.

HOW DOES THE PCI DATA SECURITY STANDARD (PCI DSS) WORK?

The PCI Security Council has defined a comprehensive security program specifying the controls and processes for organizations that wish to process credit cards. Additionally, the council defines how and when you are audited for compliance. Depending on your transaction volume, card-present or card-not-present processing (including mobile payments), and what aspects of payment processing you outsource, you will be required to implement some or all of the PCI DSS controls. Regardless of your transaction volume, or which elements of payment processing you outsource, you and your organization are ultimately held responsible for fraudulent transactions through your credit card processing agreement.

Additionally, you are responsible for upgrading your PCI controls and processes when the council upgrades the requirements. The council provides advanced notification of upcoming changes, during which time drafts are published and time is allowed for businesses to switch to the new standard. In general, two factors usually trigger a standards upgrade: (1) A breach happens, which identifies a gap or improvement opportunity in the standard; or (2) technology shifts occur, such as the adoption of mobile payments, or EMV. You can stay abreast of these changes by checking in with www.pcisecuritystandards.org at least twice a year.

SELECTING A PCI PAYMENT-PROCESSING VENDOR

Most organizations want to stay focused on building and growing the business, not learning and maintaining the intricacies of the PCI standard. Whether you are looking for a Point of Sale, online e-commerce, or mobile payment system, choosing a qualified vendor is a critical first step. In addition to verifying whether the vendor meets your technical needs, the list below provides some additional qualifying questions for a potential vendor.

1. Is the vendor certified?

The PCI council maintains a list of certified vendors. You can access the list here: Certified Vendors. However, many vendors choose not to be certified. Instead, these vendors state that they meet the PCI compliance standard in their literature and, hopefully, their terms of service.

---

[7] https://www.internetretailer.com/2015/07/29/global-e-commerce-set-grow-25-2015

2. Ask for a copy of the vendor's Report on Compliance (RoC).

If the vendor is not certified, you need to ask for evidence that shows that they meet the PCI standard. The RoC is one way to validate the vendor's claims. While most vendors won't give you the detailed report (because it includes discovered vulnerabilities), insist on an executive summary, check the date of the report, and ask them to verify that they have remediated any findings in the RoC.

3. Will the vendor indemnify you?

Indemnification is a crafty legal term, but in this case it is important. In general terms, your business needs the PCI vendor you select to indemnify you if a PCI data breach occurs because of a problem in their system. Earlier, we said your business is ultimately responsible for any data breach. Even if the vendor is at fault, you will incur expenses due to the breach. Indemnification is a way to have them cover your costs. Of course, the vendor needs to be financially sound to meet these obligations.

4. Does this vendor have good engineering management?

Can this vendor keep up with changing PCI standards? Have they considered how to update physical systems, such as PoS or mobile terminals? While it may seem easier to update a SaaS solution, there needs to be a sandbox environment and an easy mechanism for you to test any upgrades before you migrate.

5. Does the vendor have a sound business continuity and disaster recovery plan?

If you are going to partner with a vendor for a critical aspect of your business, you need to be comfortable with their ability to recover from unexpected outages. While it is not always possible to run a real simulation, you can and should ask potential vendors about the worst situation they have had to manage, and whether or how they run internal assessments. Ask online providers to fill out the Cloud Security Alliance questionnaire, or at least the sections of it you find relevant to your business. CSA Questionnaire

PCI PAYMENT-PROCESSING AUDITING AND SELF-ASSESSMENT FOR E-COMMERCE

The PCI Security Council divides merchants into categories by transaction volume and cardholder data exposure. Deciding which category you belong to determines what type of report and auditing you need.

Large merchants:

If you process a large number of transactions (about 1 million per year over any acquisition channel), you are going to need an annual RoC issued by a certified assessor. You can find a list of assessors here: Qualified Assessors

Everyone else:
Most small to medium businesses will either fall below the transaction volume or completely outsource their cardholder processing. Therefore, you can self-assess your environment against a set of questionnaires mandated by the PCI council. Most of the self-assessment categories are straightforward. You can read them here: PCI Self Assessments. However, there is a subtle difference for card-not-present-only merchants, and it relates to the level of control you have over the data entry mechanism for cardholder data. There are two self-assessment choices:

A – For merchants that do not store, process, or transmit cardholder data. This questionnaire applies when you completely outsource, via an iframe, for example, or by transferring the call for telephone orders.

A-EP – Applies when part of the cardholder data is processed by you. For example, if you build a form on your site where users enter cardholder data and then transmit that form to a payment processor. Even though the cardholder data is never stored on your system, the mere act of intelligently gathering the data from the user puts you in this category.
All of the self-assessment forms are going to ask you questions that are designed to validate you have implemented the 12 PCI security requirements, which are listed at the end of this paper.

PCI RISK

The introduction of EMV in card-present transactions potentially increases merchant risk. Essentially, in card-present transactions, if you accept a counterfeit chip-enabled card because your business only supports magnetic stripe processing, as the merchant, you may be liable for the chargeback[8].

The second risk associated with PCI is data breach. While the press is full of news about big merchant data breaches, all businesses are vulnerable. The best way to avoid such risk is to design your payment processing on a completely separate network, virtual or physical, from the rest of your systems. As this is rarely practical, the following tactics, in addition to the 12 PCI requirements, are recommended:
1. Use network configuration management tools to build one-way network diodes to ensure cardholder data never leaks off the PCI-scoped network. It is tempting to assume that a firewall is the only tool needed to ensure network security, however, temporary routes can become accidentally permanent, and new devices can be misconfigured, leading to alternative network paths that allow data exfiltration. Using good network configuration tools can help your organization maintain proper network flows.

---

[8] http://www.emv-connection.com/downloads/2015/05/EMF-Liability-Shift-Document-FINAL5-052715.pdf

2. Use network monitoring tools to ensure that no unusual protocols are operating on the PCI-scoped network. This ensures that data exfiltration will not happen over protocols such as DNS or IRC.

3. If you are in the United States, reach out to your local FBI team. The FBI is very involved in helping businesses combat cyber crime. Whether it's an advance warning, or post-breach assistance, the FBI employs teams of trained and knowledgeable experts who can help your business maintain security and compliance. You can find your local FBI office here: FBI Field office search

The above suggestions are extraneous to proper implementation of the PCI requirements. Failure to correctly implement the PCI controls can lead to civil liability in some jurisdictions. In the United States, for example, Nevada has included PCI controls in their state business statutes[9], and other states have adopted parts of the PCI requirements, or are considering doing so.

THE PCI DSS 12 CONTROLS

The good news about the PCI controls is that they form an excellent basis for any security program, and you have probably already implemented most of them. Divided into six domains, the controls are listed below. If you are musically inclined, the PCI council has created a video that summarizes the requirements. You can view that here: PCI Requirements Rock.

Remember, the most challenging part of a PCI program is scoping. If you add payment processing to an existing system, it's hard to limit where the cardholder and PAN data travels. This leaves all your systems and networks in scope and subject to the PCI requirements.

BUILD AND MAINTAIN A SECURE NETWORK

Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

PROTECT CARDHOLDER DATA

Requirement 3: Protect stored cardholder data.

Requirement 4: Encrypt transmission of cardholder data across open, public networks.

MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

Requirement 5: Use and regularly update anti-virus software.

Requirement 6: Develop and maintain secure systems and applications.

---

[9] http://www.leg.state.nv.us/nrs/nrs-603a.html

IMPLEMENT STRONG ACCESS CONTROL MEASURES

Requirement 7: Restrict access to cardholder data by business need-to-know.

Requirement 8: Assign a unique ID to each person with computer access.

Requirement 9: Restrict physical access to cardholder data.

REGULARLY MONITOR AND TEST NETWORKS

Requirement 10: Track and monitor all access to network resources and cardholder data.

Requirement 11: Regularly test security systems and processes.

MAINTAIN AN INFORMATION SECURITY POLICY

Requirement 12: Maintain an information security policy.

SOLARWINDS LOG & EVENT MANAGER

SolarWinds® Log & Event Manager is an affordable, award-winning SIEM solution that produces out-of-the-box compliance reports for PCI. Log & Event Manager can be installed in minutes, and easily generates compliance reports quickly using audit-proven templates.

NEXT STEPS

1. Download and read the Using SolarWinds Log & Event Manager to Meet PCI Requirements white paper. This white paper discusses each of the 12 PCI requirements and how SolarWinds Log & Event Manager can help you meet these requirements in an efficient, cost-effective manner.

2. Try SolarWinds Log & Event Manager for yourself. Download a free 30-day trial and have it up and running in about an hour.

Log & Event Manager is the fast and easy way to PCI compliance reporting.

ABOUT SOLARWINDS

SolarWinds provides powerful and affordable hybrid IT infrastructure management software to customers worldwide, including Fortune 500® enterprises, small businesses, government agencies, and educational institutions. We are committed to focusing exclusively on IT pros, and strive to eliminate the complexity that they have been forced to accept from traditional enterprise software vendors. Regardless of where the IT asset or end-user sits, SolarWinds delivers products that are easy to find, buy, use, maintain, and scale, while providing the power to address all key areas of the infrastructure from on-premises to the cloud. Our solutions are rooted in our deep connection to our user base, which interacts in our thwack® online community to solve problems, share technology and best practices, and directly participate in our product development process. Learn more today at http://www.SolarWinds.com/.