NACS/PCATS WeCare© Data Secuirty Program Overview

February 29, 2012

Abstract

This document describes the WeCare© Program, discusses common data security threats, outlines an 8-point plan to improve data security, and provides the reader with additional resources for risk reduction.

Contributors

Brad Cyprus, Vendor Safe Technologies
Ernie Floyd, Radiant Systems
Shekar Swamy, Omega ATC

Revision History

Revision Date	Revision Number	Revision Author	Revision Changes
Feb 29, 2012	Draft 0.5	Linda Toth, PCATS	Updated contributors and resource sections
Feb 17, 2012	Draft 0.4	Linda Toth, PCATS	Standardize format, improve readability
Jan 6, 2012	Draft 0.3	Brad Cyprus, Vendor Safe Technologies Shekar Swamy, Omega ATC	Initial Revision

Copyright Statement

Disclaimers

The National Association of Convenience Stores (NACS), Petroleum Convenience Alliance for Technology Standards (PCATS), participating vendors and retailers make no warranty, express or implied, nor do they assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product, or process described in these materials.

1 Introduction

Level 4 merchants are defined by Visa as those merchants who process less than one million Visa transactions annually. Because the cost of a data breach can be significant, a large number of these merchants, primarily single store operators, face the challenge of reducing the risk of a data breach. Low levels of data security increase the potential for data breach incidents.

The goal of the NACS/PCATS WeCare© Data Security Program is to define a risk reduction program for small operators that is easy to implement and achieves a base level of data security without incurring significant costs. Members of the PCATS Data Security Committee developed this program based on their combined experience in data security and c-store operations.

2 Common Threats

Small operators who have installed POS and back office systems with broadband communications are able to serve customers more efficiently by quickly processing credit card transactions. With the improved capabilities comes a host of threats that require management. The major threats include:

- Weak Remote access and remote control practices that leave the backdoor open
- Use of common passwords and common accounts
- The failure to install and maintain a certified Payment Application resulting in a vulnerable payment environment
- Over reliance on third-parties to install and manage POS System and not managing risks properly
- Lack of an anti-malware program designed to trap and contain viruses and other malicious software on an ongoing basis
- Lack of installed firewall with proper network segmentation
- Failure to check for overlays on pin pads at the pump to prevent skimming

Any one of these threats can easily lead to a data breach. Properly managing these threats requires an ongoing commitment by the store operator. As technology and operating conditions change and evolve, review is necessary to ensure that security measures remain in place.

3 NACS/PCATS WeCare© Data Security Program

This program can assist you in achieving a baseline level of data security. If you follow these simple guidelines and best practices, you can significantly reduce your risk. Over time, you may then be able to incorporate an even higher level of data security than contemplated by this program, so that you will be able to achieve measurable compliance to other industry security standards. The purpose of this program is to help

you get started with security so that you will at least mitigate the most common areas of vulnerability.

The WeCare© Program includes Guidance Documents and Best Practices to address several types of threats. It also includes education and webinars tailored to meet the needs of Level 4 merchants.

4 The 8-Point Data Security Plan

Below are the essential elements of data security for your retail sites:

1. Run a certified payment application (PA-DSS validated)
Verify that your POS applications are running the current certified versions. There are published lists of approved POS versions that you may refer to or ask your vendor to provide you with documentation. Check the version of your application periodically to verify that it is still in the approved list.

2. Keep your PA-DSS Validated Application Patched and Current
Apply recommended patches to your systems and update your POS application to keep them current. If your POS vendor upgrades your POS applications, verify that it is an approved version that is also PA-DSS validated. It is always a good idea to check every POS machine.

3. Install a hardware firewall with adequate network segmentation
This important requirement ensures that access to your store network is protected from outside intrusion. Segmentation further improves data security by keeping your POS systems separate from other systems. To be sure, you need to examine the configuration of the firewall frequently to ensure that no one has changed the security after installation.

4. Use only secure, two-factor authenticated remote access and remote control
Ensure that anyone who is accessing your systems from the outside is using two forms of authentication to uniquely identify each individual. This requires something known and something physical that validates someone's identity. For example, using a password could be something known, and having a soft token or a key fob could be something physical. Keep in mind that the remote control program itself should also support encryption. Knowing who is accessing your systems and when they are accessing them is one of the easiest ways to maintain security.

5. Change default passwords and have unique accounts for each user
Ensure that every POS and back office machine account password is changed frequently. The account name has to be unique for each user - although users often pick their own passwords.

6. Run anti-virus or white listing software
All systems at your stores must have a good Anti- Virus program, which is frequently updated with the latest signature files. You need to run the scans daily and ensure that you are looking at the results of the scans. Anti-Malware programs are often separate from Anti-Virus and it would be a good idea to use it as well. You may use white listing software to limit your systems to run only authorized programs. This is an alternative to Anti-Virus because it will block viruses from being able to install themselves onto a system, but white listing software will require time and expertise to configure.

7. Do not allow open access to websites from your POS systems
Segmentation of the network can limit the POS network from the Internet while still allowing access to the Internet from other stations that are not accepting payments. Also, change the settings on your POS systems to ensure there is no way to surf the web. The only exceptions should be to the approved Anti-Virus update sites and any other logging site for the POS security logs. Disallow everything else.

8. Run external vulnerability scans on the site to identify vulnerabilities and be committed to spending the time it takes to mitigate the gaps found.
Performing external scans quarterly will enable you to know how secure your retail site is from the outside. The purpose of the scans is to verify that a hacker on the Internet looking for vulnerable sites will not find any opening into your network from the Internet. Fixing security issues found after a scan will make your retail site more secure.

Data breaches at retail locations can be greatly reduced by following the eight points defined above. NACS and PCATS are committed to providing you guidance, education, and best practices to help you in reducing your risk. Data Security is the foundation on which you can build a compliance program.

5 Additional Resources

PCATS guidance documents are available on their website (http://www.pcats.org/wecare) as follows:

1. PCI Convenience Store Employee Data Security Training Manual
   This document provides example training and discussion points for use with your store employees to prevent and reduce payment card fraud and security breaches of card data. It also reviews the steps you can take to discourage and reduce theft of card data at your dispensers.

2. Guide to Simple Network Design
   This document provides guidance on simple network design for typical C-Store environments. In addition, this document provides discussion points for consulting with a network or data security professional.

   C-Store operators are typically non-technical people and network design can be very confusing. To that end, PCATS is offering some very simple designs that locations

can use when talking with third parties about network attached systems, configuration of those systems within the store, and the ability to meet the criteria set for security for a level 4 merchant under the PCI Data Security Standards (PCI-DSS).

The target audience for this document is the C-Store owner who has no or limited Information Technology (IT) network and security resources. While we expect that C-Store owners are level 4 merchants, this guidance is applicable for all C-Store owners, regardless of actual merchant level.

3. Guide to Remote Access Management
   This document provides guidance on protecting Convenience Store systems by deploying and using Secure Remote Access Management practices to thwart undesirable access that would compromise cardholder data. It provides a discussion on best practices for Remote Access Management. Each covered topic provides a summary that addresses the high level points, followed by details that allow the reader to dive deeper into the technology specifics

   The target audience for this document is the C-Store owner who has no or limited Information Technology (IT) network and security resources. While we expect that C-Store owners are level 4 merchants, this guidance is applicable for all C-Store owners, regardless of actual merchant level.

Small chains and single site operators often lack the expertise, resources, and/or time to deal with data security. Several vendors who are members of NACS and PCATS are available to help you through the process. They deal with these issues every day for retailers just like you. Contact PCATS (email: info@pcats.org) for additional information.