NACS/Conexxus WeCare© Data Security Program Overview

October 10, 2015

Version 1.1

Abstract

This document describes the WeCare© Program, discusses common data security threats, outlines a 9-point plan to improve data security, and provides the reader with additional resources for risk reduction.

Contributors

David Bones, Vendor Safe Technologies
Mark Carl, EchoSat
Ernie Floyd, Radiant Systems
Kimberly Ford, Valero
Kara Gunderson, CITGO
Steve Reischman, Heartland Payment Systems
Phil Schwartz, Valero Energy
Robert Slimmer, BP
Shekar Swamy, Omega ATC
Linda Toth, Conexxus

Revision History

Revision Date	Revision Number	Revision Editor(s)	Revision Changes
October 10, 2015	Draft 1.0.2	Mark Carl, EchoSat Kara Gunderson, CITGO Kimberly Ford, Valero Steve Reischman, Heartland Payement Systems Robert Slimmer, BP Linda Toth, Conexxus	– Updated for additional guidance and error corrections
Apr 8, 2014	1.0.1	Linda Toth, Conexxus	– Updated for Conexxus
Mar 27, 2012	1.0	Linda Toth, PCATS	– Corrected minor grammatical and spelling errors
Mar 12, 2012	Draft 0.6	Linda Toth, PCATS	– Updated contributors, original editors and resource sections – Added note that implementing the 8 points does not guarantee compliance with any particular security mandate
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	David Bones, Vendor Safe Technologies Shekar Swamy, Omega ATC	Initial Revision

Copyright Statement

Disclaimers

NACS, Conexxus, 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. Although Conexxus uses reasonable best efforts to ensure this work product is free of any third party intellectual property rights (IPR) encumbrances, it cannot guarantee that such IPR does not exist now or in the future.

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/Conexxus 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 Conexxus Data Security Committee developed this program based on their combined experience in data security and c-store operations.

2 Common Vulnerabilities

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 vulnerabilities that require management. The major threats include:

- Weak remote access and remote control practices that leave the back door 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 an installed firewall with proper network segmentation;
- Failure to check for overlays on pin pads inside and at the pump to prevent skimming;
- Lack of monitoring and alerting for critical systems within the cardholder data environment; and
- Lack of effective training and security practices, policies and procedures for employees.

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/Conexxus 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. However, implementing these steps alone does not meet any particular security mandate or standard, including but not limited to, PCI-DSS compliance. Over time, you may 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 9-Point Data Security Plan

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

4.1 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, major oil brand or acquirer/processor to provide you with documentation. Check the version of your application periodically to verify that it is still in the approved list. Validate which components are part of the PA-DSS application, and which components are your responsibility to maintain and monitor.

4.2 Keep your PA-DSS Validated Application Patched and Current

Apply recommended patches to your systems and update your POS applications 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. See Section 5 Additional Resources for additional information on where to find a list of PA-DSS validated payment applications.

4.3 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. Permitting only necessary inbound and outbound traffic helps to minimize risk associated with malicious activity. To be sure, you need to examine the configuration and rule sets of the firewall frequently to ensure that no one

has changed the security. Monitor the firewall logs for abnormal activity that might indicate a breach of internal systems, or outsource monitoring, logging and alerting to a compliant service provider. Verify that remote vendor access through the firewall to POS components is enabled only when needed, and turned off when not in use.

4.4 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, including the POS vendor if you have provided them with remote access, or if the POS system implements its own remote access. This requires something you know and something you have that validates your identity. For example, using a password could be something you know, and having a soft token or a key fob could be something you have. Keep in mind that the remote control program itself should also support industry-accepted encryption. Knowing who is accessing your systems and when and how they are accessing them is one of the keys to maintaining security.

4.5 Change default passwords and have unique accounts for each user

Ensure that every account password for every device within the cardholder data environment is changed frequently, at least every 90 days. The account name has to be unique for each user - and users should be required to pick and maintain their own passwords. For administrative accounts with high levels of access, it's particularly important to make sure those accounts have very strong passwords, using combinations of lower and upper case letters, numbers and special characters.

4.6 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 from the application vendor. 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 is recommended to use one as well. You may use white listing software to limit your systems to run only authorized programs. This is not an alternative to Anti-Virus programs, since viruses can be introduced directly to your systems regardless of white listing.

4.7 Do not allow open access to websites from your POS systems

Segmentation of the network should restrict the POS network from general Internet access while still allowing access to the Internet from other systems that are not accepting payments. Also, change the settings on your POS systems and firewall to ensure there is no way for the POS systems to access the Internet, except for those necessary to allow encrypted communications for payments. The only exceptions should be to the approved Anti-Virus / Anti-Malware update sites and any other logging site used for the POS security logs. Disallow access to all other Internet destinations from the POS systems.

4.8 Run external and internal vulnerability scans on the site to identify vulnerabilities and be committed to spending the time it takes to mitigate the gaps found.

Performing external and internal scans quarterly will enable you to know how secure your retail site is from the outside, and from inside systems that might have been compromised. 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, or from internal systems that they might have gained access to. Fixing security issues found after a scan will make your retail site more secure. For systems that require outside access, such as video security and tank monitoring, limit the remote access to only locations that need it, instead of allowing access from anywhere on the Internet. When possible, use VPNs to grant access to these systems instead of port forwarding on the site's firewall, which could cause external vulnerability scans to fail.

Data breaches at retail locations can be greatly reduced by following the eight points defined above. NACS and Conexxus 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.

4.9 Train employees on security best practices, as well as policies and procedures.

Retail locations are susceptible to a number of types of breaches, which include physical breaches of equipment both inside and outside the store. Skimmers can be placed in pumps to skim and collect card numbers, and intruders can breach network equipment if they gain access to it inside the store. It's important to train all employees, including clerks, to be aware of those areas that are susceptible to breach, what to look for, and when to notify management of potential intrusions.

5 PCI-DSS section 12.6 requires that a formal security awareness program be in place for merchants. This program should include training for employees on what to look for at individual sites that might indicate an intrusion has occurred. Additional Resources

A number of resources are available to help you with data security. These include implementation guides from your payment network provider and POS vendors, as well as educational and technical documents from various organizations such as card merchants, data security standards bodies, and government agencies.

For a complete listing of PA-DSS Validated Payment Applications, visit the PCI-SSC website at https://www.pcisecuritystandards.org.

Card Brand Resources:

https://usa.visa.com/support/small-business/fraud-protection.html
https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations.html
https://www209.americanexpress.com/merchant/services/en_US/data-security
https://www.discovernetwork.com/merchants/fraud-protection/index.html

In addition, Conexxus has put together guidance documents, which are available on their website (http://www.conexxus.org/wecare) as follows:

5.1 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.

5.2 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, Conexxus 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.

5.3 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 Conexxus are available to help you through the process. They deal with these issues every day for retailers just like you. Contact Conexxus (email: info@conexxus.org) for additional information.