Remote Access Compliance & Responsibilities

December 21, 2017

Version 1.0

CONEXXUS
solve forward

Document Summary

This paper is written to help educate and inform the retail petroleum industry store operator/small merchant about cybersecurity issues and to help raise awareness about the importance of these issues. It discusses the impact of cyber attacks and the responsibilities of the store operator for the security and compliance of store computing systems, networks, and data with applicable industry standards.

Contributors

Alan Thiemann, Conexxus
Allie Russell, Conexxus
Bob Slimmer, BP
Bradford Loewy, Wayne - Dover Fueling Solutions
Branden Williams, First Data
Brian Russell, Verifone
Bruce Welch, Gilbarco
Chris Lietz, Coalfire
Chuck Young, Impact 21
Cory Schlegel, Petrosoft
Dan Fritsche, Coalfire
Danny Harris, Security Innovation
David Creps, ExxonMobil
Dean Meckelburg, ExxonMobil
Don Emory, CHS
Doug Spencer, NACS
Ed Kelb, Verifone
Gray Taylor, Conexxus
Jake Hoxha, Excentus
Jeff Gibson, ControlScan
Jim Sheppard, Phillips 66
Kara Gunderson, Citgo
Keith Hess, Alon
Kim Seufer, Conexxus
Kimberly Ford, Valero
Linda Toth, Conexxus
Mark Carl, ControlScan
Matt Bradley, ControlScan
Mike Lindberg, CHS
Monier Jalal, Cybera
Nancy Tosto, BP
Nunu Ladek, ExxonMobil
Paul Melton, Cybera
Raymond Prothero, Verifone
Ron Hilmes, Chevron
Sam Pfanstiel, Coalfire
Scott Cheek, SageNet
Simon Gamble, Mako Networks
Steve Reischman, Heartland Payment Systems
Steven Bowles, Wayne - Dover Fueling Solutions
Tabitha Greiner, Acumera
Terry Mahoney, W Capra
Vidya Swamy, Omega ATC

Revision History

Revision Date	Revision Number	Revision Editor(s)	Revision Changes
December 21, 2017	Version 1.0	Linda Toth, Conexxus	Final Release Version
December 4, 2017	Draft 0.4	Linda Toth, Conexxus	Updated after SQA, TAC, and public comments received. Formatting, copyright notice changed to public facing, diagram in Appendix C updated, glossary terms updated and formatted.
October 5, 2017	Draft 0.3	Linda Toth, Conexxus	Added contributors, updated copyrights, disclaimer, cleaned up formatting, corrected spelling errors.
June, 2016 through September 2016	Draft 0.11 through 0.2	Danny Harris, Security Innovation Tabitha Greiner, Acumera	Rework with feedback from committee and legal reviews
May, 2016	Draft 0.1	Danny Harris, Security Innovation	Original work

Copyright Statement

Disclaimers

Conexxus makes no warranty, express or implied, about, nor does it 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.

This document is provided with the understanding that neither Conexxus, nor any individuals who participated in its preparation, shall be deemed to be engaged in rendering legal or technical advice and services. Therefore, this document should not be used as a substitute for consulting with competent legal or technical advisers.

Table of Contents

1 Introduction

1.1 Why Cybersecurity Matters to the Retail Petroleum Industry

Data security is necessary to our industry: it's something that customers expect and deserve; and it's something we need to provide to ensure that the data and systems we use are adequately protected from criminals. Merchants also need to consider regulatory requirements, along with federal, state and local laws, that may be applicable to your business.

1.2 Cyber vs. Physical Security

One of the factors that differentiates cybersecurity from traditional physical security is that cyber attacks can be automated and conducted remotely. Physical attacks must be performed "in person" and unfold much more slowly than automated attacks. What might be difficult to accomplish with a physical attack can often be done instantaneously or trivially in a cyber attack and conducted with much less risk to the stealthy criminal (e.g., stealing thousands of payment cards).

Although it is still necessary to have protection mechanisms in place against traditional physical crimes, it is equally critical that you adequately protect your store systems, networks, and any sensitive data (i.e., cardholder data, loyalty data, sensitive business records) from cyber criminals.

1.3 The Impacts of Cybercrime

The impacts of cybercrime can often be quite significant. For example, the diagram below shows some of the possible impacts of a cardholder data breach. You will notice there are multiple financial pain points to consider.

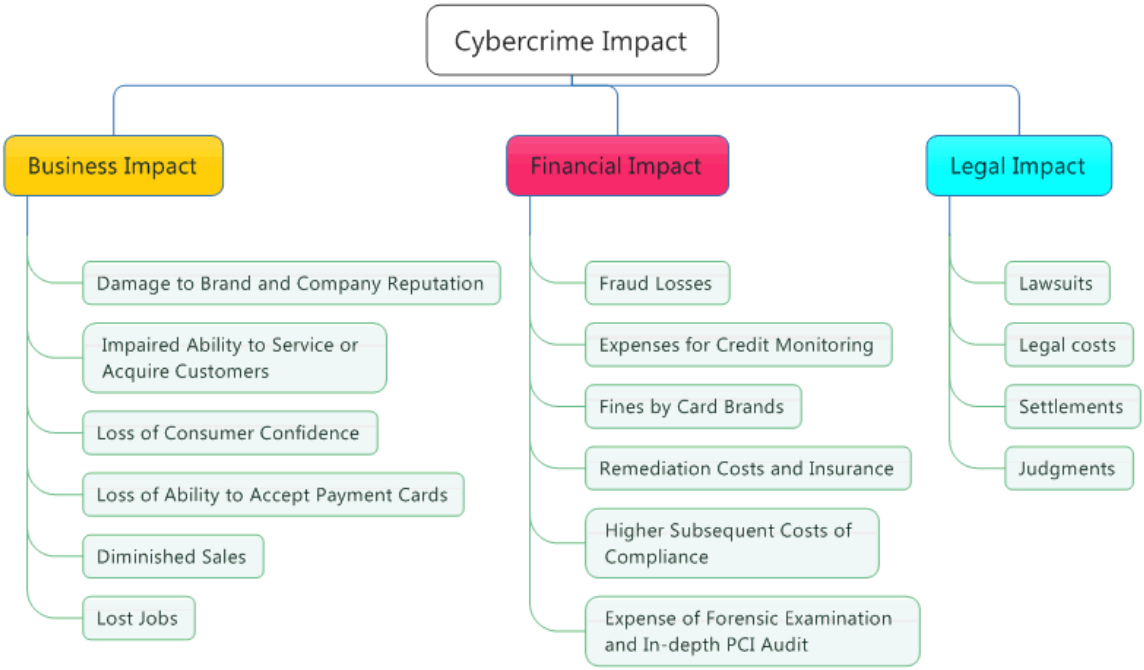


Figure 1: Possible Impacts - Cardholder Data Breach

2 The Current Threatscape

2.1 Who is a Target?

You might wonder, "Who is a target of cyber criminals?" The answer is that **everyone** is a potential target. If you have something of value, criminals are interested.

Surprisingly, smaller retail stores are often a sizeable target, since their computer systems are often poorly defended due to limited budgets, resources, and technical expertise. One of the vulnerabilities of the Internet is that it enables criminals to find these poorly defended systems rather easily, enabling attackers to go after the easiest targets first, even if it is a small store.

The Verizon Data Breach Investigations Report (DBIR) for 2016 found that there were 534 POS intrusions (525 confirmed breaches with data disclosure) and 102 Payment Card Skimmer incidents in its database of known incidents. Together, these incidents accounted for 91% of payment card breaches in its study.

Data published from Visa shows that over a period of two years, the overwhelming majority of compromise events happened at brick and mortar organizations.

These are just two examples of many showing the real risks that retailers face.

2.1.1 Your Store is a Target

Your store is a target primarily for these reasons:

- You handle or possess things that are valuable to criminals
  - Personally identifiable information which can be used for identity theft;
  - Business records (e.g., bank account statements, loan documents) may be used to conduct theft against your business;
  - Sensitive internal information that could be used to harm your business or cause havoc;
  - Payment cards have intrinsic value and can be used almost anywhere to purchase items. Stolen card data is also sold on the black market and can be used to create payment cards allowing criminals to make fraudulent purchases of physical goods.
- Your computers and networks are potentially exposed to attackers through the Internet.
- If your computer systems are not adequately protected, it can be easy for an attacker to break in and those breaches not be easily detected.

2.1.2 POS Integrators and Resellers

POS integrators and resellers are a target. Why? Criminals will try to steal the authentication credentials, which will allow the attacker to access merchant systems and networks. In some instances, integrators deploy poorly secured remote access solutions. Once an attacker finds those vulnerable systems, an attacker may be able to use the remote access solutions (provided by POS Integrators and resellers for maintenance purposes) to break into the store network and steal cardholder data, personnel data or company data.

2.1.3 Third-Parties

Third parties that provide services to you are also a target. Just like POS integrators and resellers – these companies are targeted to try to steal authentication credentials or to find paths into your systems and networks.

2.2 Common Cyber Attacks

Retailers face a variety of attacks and threats to their data. The focus of this paper is specifically on some of the more common cyber attacks. Many cyber attacks being perpetuated have common themes, such as obtaining authentication credentials and then using them through remote access systems to breach store systems. Below are some common types of cyber attacks.

2.2.1 Phishing Attacks

Phishing is an attempt to obtain sensitive information through communication methods that appear to come from a trustworthy source. For example, you may receive an email or telephone call from someone impersonating an important company officer/manager asking you to provide information for a critical project. This is a phishing attack, which is designed to trick you into clicking on malicious links, opening booby-trapped attachments, releasing secure data, or even taking specific actions (such as wiring money or issuing a corporate check). In regards to store systems, phishing attacks are often used to steal credentials that allow the attacker to login to store systems. Additionally, phishing attacks are used to get malicious software installed on systems.

2.2.2 Social Engineering

With this tactic, criminals try to trick you into giving out information or performing actions. For example, a repair technician may call you on the phone and ask for information about your location. One method to prevent this type of attack is to ensure everyone in the store knows when repairs are scheduled and setting up a legitimate contact you can call to confirm that any requests for information are real. Make sure you do not give out sensitive information to an attacker pretending to be someone else!

2.2.3 Malware Attacks

Malware is a software program that is designed to damage systems or steal sensitive data. Once a criminal gains entry into the store network, attackers will often install malware to assist in the attack and theft of data. Below are some common types of malware:

Malware Type	What it Does
POS Malware	A generic name for malware designed to collect information from POS systems. Often it is targeted to steal cardholder data from the point-of-sale terminal's computer memory. Other POS malware finds and exfiltrates the collected cardholder data.
RAM Scraper	A class of malware designed to collect and exfiltrate unencrypted data that is temporarily held in computer memory (called random-access memory or RAM).
Backdoor	Allows the attacker unimpeded access to a computer system by bypassing security controls.

Malware Type	What it Does
Sniffer	Scans the store network traffic for sensitive data and passwords and sends them to the attacker.
Keystroke Logger	Captures all keystrokes typed by personnel, allowing attackers to steal sensitive data and usernames/passwords entered into store computer systems.
Command and Control software	Used by attackers to maintain communications with compromised systems within a target network. Generally, exfiltrated data is sent to a Command and Control system operated by the attacker.

Because technically sophisticated cybercrime gangs often customize these cyber weapons, detection rates for newer malware by anti-virus software is low. This increases the likelihood of an attacker remaining undetected on store systems and networks for a longer period before they are discovered. These cyber weapons are readily available on underground black markets, and often come with training and support!

2.2.4 Remote Access Attacks

Cyber criminals also use stolen or easily guessed login credentials to login remotely to the store's computer systems and networks. The criminals can use these credentials on the remote access systems used by third parties to maintain store systems.

3 Payment Card Industry Compliance

3.1 Security and Compliance

Your first responsibility is to ensure that your systems and data are adequately protected from all types of criminals. Because payment card information is sensitive, it's necessary to ensure the security and privacy of that data.

3.1.1 Payment Card Industry (PCI) Compliance

The Payment Card Industry Security Standards Council (PCI SSC) has developed requirements related to payment card industry compliance along with associated technical and operational requirements. These requirements apply to all entities involved in payment card processing and to any entities that store, process, or transmit

cardholder data (CHD) and/or sensitive authentication data (SAD). Compliance with PCI requirements is mandatory for petroleum merchants who accept major credit cards. While PCI DSS compliance is only required for systems deemed in-scope, the types of security controls described may be useful for other systems at your site(s).

3.1.2 Why Compliance is Important

While compliance doesn't guarantee absolute security, or make you immune to attacks, compliance mandates are based on best practices and will ensure that a reasonable level of security is being achieved – and it is then up to each individual organization to determine if greater security controls are needed to get their systems to a level of acceptable risk. If your systems and data meet or exceed the PCI requirements, it will be much harder for a cyber criminal to execute a successful attack.

3.1.3 Failure to Comply with the PCI Data Security Standard

There are several potential liabilities a merchant can face for failing to comply with the PCI Data Security Standard. The impact can be very significant and costly.

In addition to the issues associated with cybercrime breaches discussed previously, there may be additional consequences, such as being assessed fines or having the company's ability to processes credit and debit cards put at risk.

3.2 Responsibility for Cybersecurity at the Store

3.2.1 Accountability and Responsibility

The merchant (the store owner/operator) is ultimately accountable for the security and compliance of its stores. Given the complexity of the store-computing environment, it is understandable that a merchant may want to outsource the installation and maintenance of systems to vendors that have the expertise; however, it is important to realize that the ultimate accountability for the security and compliance for those systems cannot be outsourced. The merchant is still ultimately accountable for ensuring that security and compliance is maintained, and this means engaging with your vendors and third-party service providers to make sure they have the knowledge to do what is necessary. Thus, it is important that you pay careful attention to the legal contracts you have with any third party, especially any vendors or service providers, so that if you are attempting to delegate responsibilities for security and/or compliance with PCI requirements, such delegation and any related issues (e.g., indemnification) are clearly spelled out.

3.2.2 Roles and Responsibilities

Recognizing that you are ultimately accountable, the following are some general criteria for determining roles and responsibilities for your systems and networks:

The responsible party is the entity who will complete the tasks and maintain processes. This will vary based on the site(s) brand, equipment, and systems installed in the store. The responsible party can be you (the merchant), the oil brand, or responsibility may be delegated to the equipment provider, the POS vendor, reseller, integrator, or service provider. If the delegated responsible party is an external entity, they will be accountable to you, the merchant, for delivering what they are responsible for, but the merchant still has overall accountability. In any given environment, you could have many different parties responsible for doing different things. That is why it is so important to have a clear understanding of the roles and responsibilities. You should have legal contracts in place to ensure that any vendors, service providers, or other third parties know and understand their responsibilities, and that they will indemnify you for any damages that are the result of their failure to take the required security actions for which they are responsible.

Ask these outside parties what their responsibilities are and what your responsibilities are in regards to technologies at your site(s). Often times the responsibilities may be shared between multiple parties.

Understanding the responsibility and accountability for the systems, network, and data in the store can be hard due to the complexity of the systems. Despite that complexity, the merchant is still ultimately accountable and that means developing a minimum level of understanding.

If you are working with an oil brand, ensure you are familiar with your contract details. Some oil brands may have recommended vendors or service providers. Some oil brands may require the use of specific vendors or service providers. While other oil brands may resell services directly.

3.2.3 Documenting Responsibilities

Is it recommended that you document each of the responsible parties and their specific responsibilities for technologies at your site(s). An example can be found in the PCI SSC's guidance document entitled "Third-Party Security Assurance and Shared Responsibilities."

Additionally, the PCI DSS has specific requirements in regards to documentation of responsibilities, such as: maintaining a written agreement acknowledging responsibility

and maintaining information about which PCI DSS requirements are managed by you and which are delegated and managed by vendors or service providers. The PCI DSS standard also requires proper due diligence prior to engaging with third-parties and the establishment of a program to monitor the PCI DSS compliance of all associated third-party service providers with whom you share cardholder data or that could affect the security of cardholder data.

4 Understanding Your Technologies

Part of understanding your own site(s) is getting to know the basics of the applications, computer equipment and networks you use. While you do not need to become an expert, having foundational knowledge of your store systems and knowing where to go to get answers to questions is important. Make sure you know who your vendors and service providers are and have their current contact information.

You should develop an equipment inventory for your store. An example way to build and communicate site asset data can be found in the the Conexxus Site Asseset Standard. (See Appendix B).

Here are some examples of technologies that might be found in a typical store. If you are unfamiliar with a piece of equipment, ask the vendor to provide the necessary information to complete the asset list. It is important at least to know what each piece of equipment looks like, where it is located, and who is responsible for maintaining it.

Computers	Fuel-Related	Security
• Desktop/laptop PCs • Servers • Personal devices – phones, tablets • Kiosks	• Fuel tank monitoring systems • Outdoor Fuel Price Signs • Forecourt fuel controller	• Alarm system • Network cameras • Video Recording System o Digital Video Recorder o Analog Recorder

POS Systems	Technologies

• POS Terminals
  o Card readers – in dispensers and standalone
  o PIN Pad with card reader
• POS Payment Application(s)
• Order confirmation display
• Printer – as part of the POS and as part of the back office PCs
• Scanner
	• Price sign with remote access and digital displays
	• Cash management system (smart safe)
	• ATM
	• Loyalty card
	• Lottery
	• Car wash
	• Scales
	• VoIP phone
	• Printers
	• IoT devices

The table below covers networking equipment, with which you may not be familiar, but is critical for the security and operation of your systems.

Network Connectivity	Network Security	Modems
• Router • Switch • Wireless Access Point (Wi-Fi) • VPN Concentrator • Satellite	• Firewall (hardware and/or software) • Security Appliance (standalone or integrated as part of another device) • Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)	• Dialup modem • Cellular data modem • Broadband modem (DSL, Cable, fiber, etc.)

An example store diagram showing how some of these systems may fit into your network is shown in Appendix C.

4.1 Knowledge About Your Site(s)

Store networks can have varying levels of complexity and expansiveness, and it is impossible to be an expert in all areas. However, it is critical that you possess some fundamental knowledge to be able to “direct the troops” to properly manage and secure your systems.

Question	Why it is Important
Have you identified all devices on the store network?	If you don't have an accurate inventory, you can't be sure systems are correctly configured and up-to-date with security patches.
Do you have a basic understanding of what each device does?	A basic understanding of the device function helps you to know (at a high-level) how your network functions.
Do you know which systems store, process or transmit cardholder data? What about other sensitive data? Who has access to this data?	Understanding which systems contain sensitive data and who has access to this data will help you ensure you have the controls necessary to protect it.
Did you know that any device could be a security risk? This includes networked devices you may not have focused on, such as printers or DVRs or tank gauges.	Because many systems are networked devices (including wireless), they can be used by attackers to infect other systems or be used to extend the footprint of the attack.
Do you have your documentation together?	Ensure you have the documentation you need to protect your systems and data. Documentation such as written procedures, contact lists, vendor implementation guides, compliance documentation, system inventories and roles and responsibilities are all critical.
Is there anything that you (the merchant) must implement that the vendor didn't, to protect your systems and data?	You need to make sure that you do your part. This Conexxus document is a good starting point to help you engage in conversations to find out who is responsible for what.

4.2 Your Responsibilities

You should know the following:

- Who provided the equipment?
- Who owns the equipment?
- Who installs the equipment?
- Who services the equipment?
- Who manages the device on an on-going basis (you, the vendor, a service provider or a combination)?
    - Are they PCI certified or otherwise aware of PCI requirements to ensure PCI requirements are met?
- Is there documentation for each device?
    - Setup
    - Maintenance
    - Attestation of Compliance/Report on Compliance
    - Payment Application Implementation Guide (PA-DSS certified applications)
- Who is responsible for...
    - Setup, installation, and configuration?
    - Changing default configurations and password?
    - Patching and updating?
    - Monitoring?
    - Alerting the proper individuals and/or government offices in the event of a breach or other unusual behavior, including meeting the deadlines for breach notification in your state?
- How is maintenance done?
    - On-site by a technician
    - Remotely
    - How will notification be done?
- Is there segmentation and restricted access?
    - Are your sensitive systems and data segmented from other systems?
    - Is inbound and outbound access restricted?
- What about logging?
    - Are the logs enabled?
    - Who has access to the logs?
    - Who is responsible for reviewing logs regularly?
- What about regular security processes?
    - Who is performing regular security processes, such as vulnerability scanning and penetration testing?
    - Does your networking configuration allow for authorized scans and audits?
- Who has access to my sensitive data?
    - Which internal employees have access to sensitive data?
    - Which external personnel have access to my sensitive data (either directly or through the ability to support the system)?

4.3 Remote Access

Many vendors and service providers use remote access solutions to provide a way of allowing an authorized representative to maintain and support systems without having to physically come on-site.

Regarding remote access at your store, determine the following:

- Which vendors use remote access to administer and maintain their systems?
- What remote access solution do they use? (You may find that different vendors may have different solutions to access the equipment or systems they are responsible for)
- Do they use unique authentication credentials for your site(s)? (This is a PCI DSS Requirement that service providers use authentication credentials that are unique to your site(s))
- Do they use multi-factor authentication? (It is a PCI DSS Requirement that multi-factor authentication is used)
- Is the remote session adequately encrypted? (This is to ensure that a criminal listening to the session cannot make any sense of it and is a PCI DSS requirement that administrative sessions use strong cryptography)
- How can you enable and disable remote access? (It s a PCI DSS requirement that remote access technologies must only be enabled when needed and must be immediately disabled after use)
- Is there sensitive data on the system that remote personnel may have access to?

4.4 POS Vendor-Supplied Networking Equipment (e.g. Router)

Some POS vendors provide networking solutions that accompany their application(s). These solutions can help with network integration, security and/or provide remote access.

It is important to remember that using a PA-DSS compliant application or point of sale solution does not automatically make your store computers or networks compliant.

The table below discusses at a high level, common types of network and remote access systems.

Equipment	Function	Myths	Use cases
Router	A hardware device that forwards network traffic to different networks or to different parts of a network.	The router provides sufficient protection against network attacks. Your vendor or installer has configured and secured your router.	Makes vendor integration easier by allowing a simple solution despite a wide variety of network configurations in different stores. The router may be used to segment the network into different security zones.
Switch	A hardware device used to connect computers and devices (printers, servers, etc.) to a network.	Your vendor or installer has configured and secured the switch.	Connecting computers and peripherals to the switch gives them access to the store network.
Firewall	Software or hardware system designed to control network traffic by examining the traffic and making decisions to permit or deny the traffic based on rules.	A firewall provides sufficient protection. Your vendor or installer has configured and secured your firewall.	The firewall is usually the first line of defense against unwanted network traffic and may be used to segment the network into different security zones.

Equipment	Function	Myths	Use cases
Security Appliance	A hardware device to protect the network. It may include firewall functionality (blocking unwanted traffic), virus protection, content filtering (blocking objectionable content), and intrusion detection/ prevention capabilities.	The security appliance provides sufficient protection. Your vendor or installer has configured and secured the security appliance.	Used to simplify care and maintenance of networks because it can handle many different functions that might be otherwise done using multiple devices.
Remote Access Solution	Hardware or software solution that allows remote users to access internal networks and computers.	The remote access solution is secure and only allows the specified person access to store internal systems. Your vendor or installer has configured and secured the Remote Access Solution.	Used by technical support staff to maintain and update systems without having to go on-site.

4.5 The Importance of the Vendor PA-DSS Implementation Guide

One of the most important tools at your disposal is the vendor PA-DSS Implementation Guide for your payment applications. This is such an important document that the PCI SSC has made it a requirement for POS vendors to provide an "Implementation Guide" to all customers with all PA-DSS certified applications. Each vendor implementation guide goes into detail about POS configurations, requirements, and may explicitly call out responsibilities, which can be very helpful in determining what you must do to ensure you application is properly implemented and supported.

The vendor implementation guide may also have important information about any networking equipment that is part of the overall solution.

In a nutshell, you need to read and understand the PA-DSS implementation guide because it can provide useful guidance regarding the installation and configuration of the equipment, as well as its maintenance. If you are using a vendor or service provider to install or maintain some devices at your site, you should make sure that their contract requires that they are configuring the devices in accordance with the installation guide.

5 Getting More Help or More Information

A primary goal of this whitepaper is to help you to understand your store's infrastructure and to facilitate conversations with the vendors and service providers that may be supporting your systems. Here are some places to get help or more information:

Ask an expert: Get help by asking an expert. It could be a PCI Qualified Security Assessor (QSA) that you bring into the store to help you understand your systems and responsibilities or perhaps some other qualified expert or consultant.

Oil brands: The oil brands are a great resource for systems that they provide or requirements they impose on you through your franchise agreement or fuel supply agreement. They have qualified tech support staff and expertise to help you untangle the complex systems found in the store.

Ask for help: In addition to reading the vendor implementation guide for systems, be sure to ask the vendor or integrator how to use and maintain the systems installed in the store.

Know who to call: In the event of a problem or unusual behavior, know who to call. This means having a contact list with name, number, and email.

PCI Security Standards: Understand your responsibilities for PCI compliance by becoming familiar with the applicable PCI security standards.

Appendix A: Glossary

Term	Definition
Cardholder Data Environment (CDE)	The people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data. (Source: PCI DSS 3.2 Glossary)
Cybersecurity	Protection of information, systems, and networks from unauthorized or accidental access, modification, and destruction
Encryption	The process of preventing information disclosure to unauthorized people by converting it into an unintelligible form that can only be reversed by authorized people that have the appropriate key
Exfiltration	The process of secretly removing data from a computer system without authorization
Firewall	Software or hardware system designed to control network traffic by examining the traffic and making decisions to permit or deny the traffic based on rules
Internet of Things (IoT)	The network of physical devices such as video and tank monitoring, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and network connectivity, which enables these objects to connect and exchange data. Each thing is uniquely identifiable through its embedded computing system but is able to inter-opearte within the existing Internet infrastructure. Typically, the IoT is one of the most vulnerable data breach points
Multifactor authentication (MFA)	The use of two or more identity factors. The evidence may include something you know (password, PIN), something you have (a token), and something you are (biometric such as a fingerprint)
PA-DSS (Payment Application Data Security Standard)	These are requirements created by the Payment Card Industry Security Standards Council (PCI SSC) that provides security and compliance guidance to software vendors that build payment applications. The goal is to develop secure applications that will be compliant with the PCI Data Security Standard.

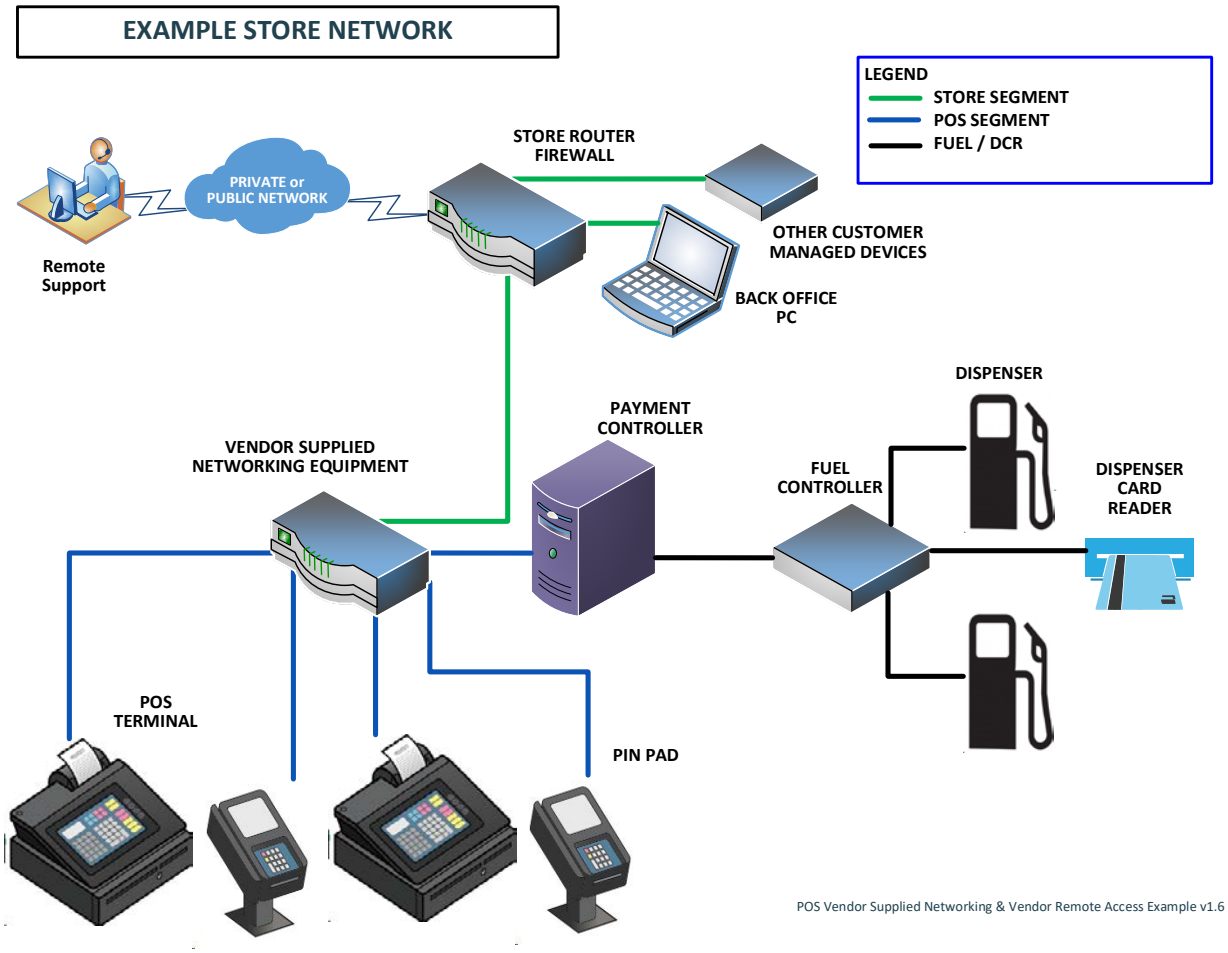
Term	Definition
PCI	Payment Card Industry
PCI-DSS (Payment Card Industry Data Security Standard)	These are information security requirements that apply to all entities involved in payment card processing, such as merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD). The goals of the PCI-DSS are to protect cardholder data, reduce the likelihood of a breach, and minimize payment card fraud.
POS Payment Application(s)	Legacy POS systems often have payment applications integrated within the overall point of sale system functionality. However, most newer petroleum POS systems segregate point of sale functionality (such as price book, scanning, etc.) from the payment application that handles the payment card functionality. Therefore, for purposes of discussion within this whitepaper, we will use the phrase "POS Payment Applications" in lieu of Electronic Payment Server ("EPS") or references to the payment application/device in association with the POS system.
Remote Access	The process of connecting to a remote computer system so that the user can interact with the system as if the user was sitting at the system itself
Router	A hardware device that forwards network traffic to different networks or to different parts of a network
Security Appliance	A device that protects systems and networks from security threats
Segmentation	The process of separating a network into distinct "segments" or isolated zones with restricted network traffic
Service Provider	Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed

Term	Definition
	firewalls, IDS and other services as well as hosting providers and other entities. (Source: PCI DSS 3.2 Glossary)
Store network	The computer network in the store. This could consist of wired and wireless networks of various types
Strong Cryptography	Cryptographic systems or components that are considered highly resistant to cryptanalysis. As an example, the PCI DSS defines strong cryptography as: *"Cryptography based on industry-tested and accepted algorithms, along with strong key lengths (minimum 112-bits of effective key strength) and proper key-management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible, or "one way")."*
Switch	A hardware device used to connect computers and devices (printers, servers, etc.) to a network
Voice Over IP (VoIP)	A methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet

Appendix B: Inventories

If you are a Conexxus member, the the Conexxus Site Asseset Standard is an example way to build and communicate site asset inventories.
https://www.conexxus.org/standards/site-asset

Appendix C: Store Diagram Example



If you need guidance on PCI DSS scoping please refer to the PCI SSC guidance document on scoping (see More Resources) or contact a Qualified Security Assessor (QSA).

Appendix D: More Resources

D.1 Payment Card Industry

PCI Security Standards Council
https://www.pcisecuritystandards.org

PCI Payment Protection Resources for Small Merchants
https://www.pcisecuritystandards.org/pci_security/small_merchant

Guidance – Third Party Security Assurance
https://www.pcisecuritystandards.org/documents/ThirdPartySecurityAssurance_March2016_FINAL.pdf

Guidance – Scoping
https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1_1.pdf?agreement=true&time=1498427586445

US Chamber of Commerce Internet Security Essentials for Business 2.0
https://www.uschamber.com/issue-brief/internet-security-essentials-business-20

D.2 Security

Conexxus We Care Program
https://www.conexxus.org/wecare

Skimming Prevention: Best Practices for Merchants v.2.0
https://www.pcisecuritystandards.org/documents/Skimming%20Prevention%20BP%20for%20Merchants%20Sept2014.pdf

D.3 Breaches and Attacks

Security Blog
http://krebsonsecurity.com

Verizon's Data Breach Investigations Report
http://www.verizonenterprise.com/verizon-insights-lab/dbir/

Trustwave Global Security Report
https://www.trustwave.com/global-security-report/

World's Biggest Data Breaches
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/