


Stronger Retail Network Security in 2017



Securing point of sale devices is part of an effective security plan, but retailers need to protect the entirety of the retail environment against sophisticated malware attacks. Explored inside is a detailed analysis of the security risks across the complex retail environment, as well as the methods retailers should be employing to ensure they have the best defense against an attack.



CONTENTS

Extending Best Practices beyond Point of Sale

How To Protect the Retail Environment

- **Mandate Point-to-Point Encryption (P2PE) for All Connections Through Your Network**
- **Segment Your Network**
 - Update software on a regular basis
 - Install firewalls and anti-virus
 - Enforce a strong password policy
- **Improve Your Security Hygiene**
 - Implement strong access control measures
 - Physically protect your systems
 - Consider contactless POS
 - Monitor and maintain system integrity

Most Importantly, Increase Security Awareness

- **Educate Your Staff and Increase Security Awareness**
 - Developing effective security awareness

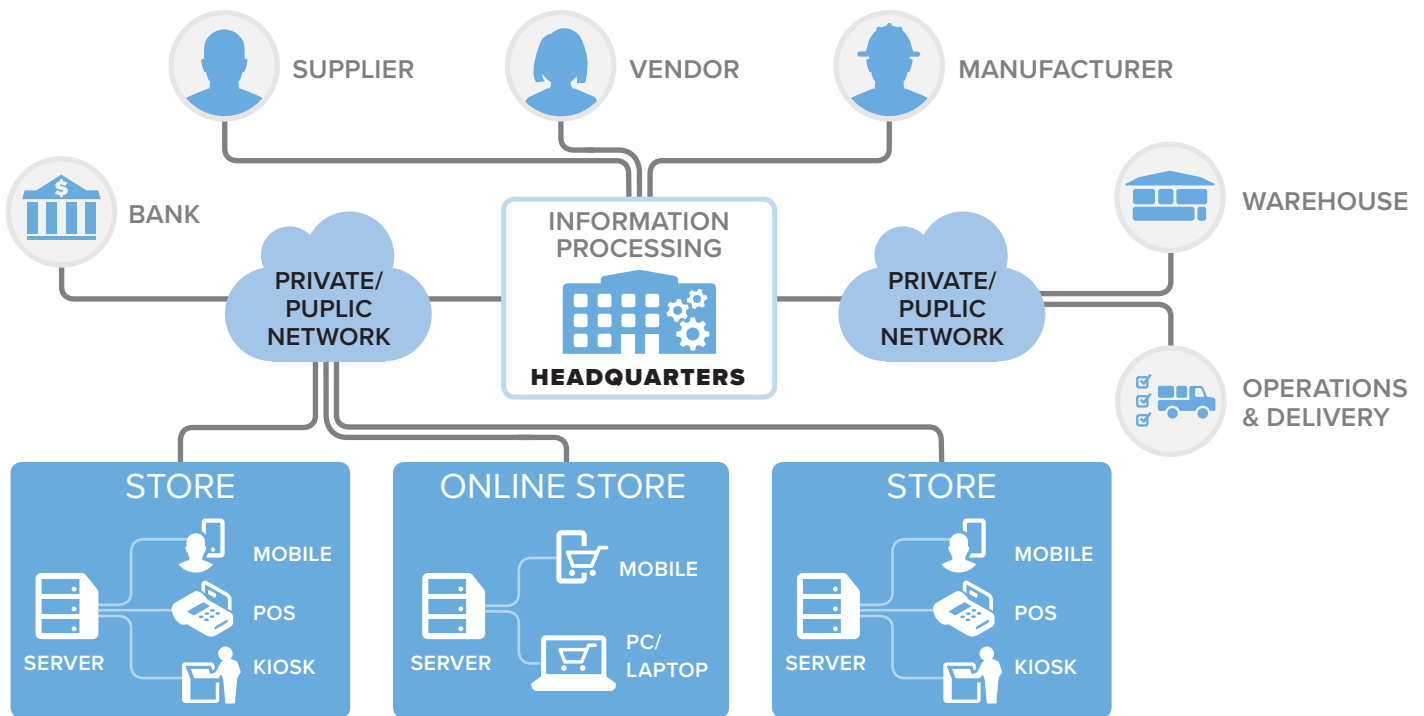
Conclusion

Extending Best Practices Beyond Point of Sale

When it comes to network security, a retailer's main concern typically lies with their point of sale systems. Because customer payment card information is gathered through POS devices, retailers naturally assume those devices will be the primary vector of any potential attack.

However, such a narrow focus deprives retailers of a holistic view of network vulnerabilities and neglects core applications and segments where much of the real danger lies.

Granted, protecting point of sale endpoints is important, yet it is only a fraction of an effective security plan. Retailers must secure the entirety of their network environment to protect their company and customers from cyber attacks.



The typical retail infrastructure includes:

- **The operational environment**
 - POS checkout terminals and peripheral devices, including self-checkout units
 - Individual PCs and back-office servers
 - Database and application servers, dedicated or sole-purpose PCs, and network devices
- **Supply chain relationships**
 - Wholesalers and distributors
 - Equipment manufacturers
 - Consultants and service providers

Many retailers operate with very low margins, often leading managers to consider network management a low priority given that it doesn't directly generate revenue. But this amounts to a lack of security visibility and coordination, making retail an attractive target to cyber criminals.

Management should keep a close eye on internal security to strengthen their value chain—on both the supply and distribution sides—as well as the security practices of staff at remote locations.

Retailers can prevent and detect cyber-attacks through understanding the vulnerabilities of the entire retail environment and following security best practices.

How To Protect the Retail Environment

While no company is ever 100% protected against cyberattacks, retailers should implement strong defenses to stop an active threat or deter would-be attackers with additional layers of security.

To close security gaps in the retail environment, always deploy multiple layers of defense.

PCI DSS Guidelines for P2PE:

- Secure encryption of payment card data at the point-of-interaction (POI)
- P2PE-validated application(s) at the point-of-interaction
- Secure management of encryption and decryption devices
- Management of the decryption environment and all decrypted account data
- Use of secure encryption methodologies and cryptographic key operations, including key generation, distribution, loading/injection, administration and usage.

*Payment Card Industry (PCI)
Point-to-Point Encryption (P2PE),
Frequently Asked Questions
(FAQs)*

Mandate Point-to-Point Encryption (P2PE) for All Connections Through Your Network

P2PE helps retailers reduce the cost of meeting PCI DSS requirements. From the moment a payment card is swiped, the card data is encrypted with the Triple Data Encryption Algorithm (TDEA) until it reaches the secure third-party server, at which point it is decrypted for authorization. To be truly protected, use P2P whenever possible throughout the rest of the network – even in devices that are considered out of scope for PCI.

Segment Your Network

“Network segmentation can be achieved through a number of physical or logical means, such as properly configured internal network firewalls, routers with strong access control lists, or other technologies that restrict access to a particular segment of a network.” – PCI DSS v3.2

Securing and segmenting the POS network from user traffic creates an extra layer of security that attackers must bypass.

Network segmentation should be used to separate different types of devices and their associated users. For example, building systems should be separate from office systems, and both should be separate from POS systems. Locate all the external-facing devices within a DMZ to secure external traffic to the local area network.

Update software on a regular basis

Because systems are more susceptible to malware and viruses if software patches are not installed, schedule regular software updates at least once a month. Beware that software updates may cause POS systems to run slower than usual during installation, so perform these scheduled updates when the business is closed.

Install firewalls and anti-virus

Install and maintain firewalls and regularly update anti-virus to protect cardholder data against malware.

Contrary to conventional wisdom, firewalls do not only monitor and control external traffic to the Internet, but can be also configured to manage internal traffic between network segments, adding a new layer of security.

Use multiple firewalls to create a perimeter network. Having all your external-facing devices located within the perimeter network allows you to better secure your internal local area network (LAN) from other untrusted networks. Configure the first firewall to allow traffic to the perimeter network only and the second one to allow traffic from the perimeter network to the LAN.

For even higher security, implement security controls with the appropriate firewall rules to permit the access specific to each of the LAN segments.

Enforce a strong password policy

Simply maintaining good password practices improves your chances against cyber criminals. Use passwords with a minimum of eight characters, including a combination of letters, numbers, and symbols. Many default passwords of common systems are well known, so require and enforce strong and unique passwords throughout the entirety of the retail environment, including third-parties and vendors in the supply chain.

Improve Your Security Hygiene

Once you have secured the Card Data Environment, implement additional security measures to prevent stolen identity and access privileges.

Implement strong access control measures

Preventing stolen access credentials through strong authentication methods will deter hackers from targeting your business.

Enforcing this PCI requirement outside the PCI zone is still a good idea. Each zone should have its own roles, privileges and access, effectively restricting user access to data within their area of responsibility and eliminating the risk of cyber criminals breaching the retail system.

1. Manage user roles and privileges

Once a user has been set up with secure access credentials to a device or application, controlling their access privileges is critical. The more granular the authorization settings, the better security you are allowed.

2. Implement strong authentication methods

Exploiting a weak or non-existent password is one of the first steps cyber criminals take to compromise a network, so retailers must implement reliable processes for authentication management.

Go beyond generic authentication methods that are vulnerable to brute force attacks and protocol “sniffers”. Instead, consider the following:

- **Smart card authentication.** Using this method, all information is processed on the card itself in rather than being transmitted to another device. The attacker must both possess the card and know the PIN number to compromise the data.
- **Biometric authentication.** Biometric authentication includes fingerprint readers, facial recognition, iris scanning, and voice identification. Fingerprint recognition is the most accessible way retailers can take advantage of biometric security at a low cost.
- **Digital certificates.** Issued by a trustworthy authority, digital certificates are used for authenticating and securing communications, especially on unsecured networks. They work by assigning a public key to a user who has the corresponding private key.

PCI DSS REQUIREMENT 7

mandates restricted access to cardholder data by business “need to know” within your organization:

- Grant access to retail system components based on job responsibilities.
- Use an automated mechanism to monitor and restrict access and privileges.
- Document all security policies in use, train your personnel, and evaluate their security awareness.

3. Enforce strong authentication for remote access and support

Most technicians and network administrators within retail will update, audit, and support POS systems from remote locations. The basic methods for strong authentication of a remote user are:

- **Multi-factor authentication.** This requires two or more forms of authentication for higher-risk access. Multi-factor authentication uses one piece of information the user knows (log-in credentials), as well as something the user possesses (passcode received by phone or email).
- **Authentication against RADIUS.** RADIUS is a client/server protocol often used to centrally validate remote users and authorize their access to network resources. RADIUS integrates well with VPN, RAS, Active Directory and Token based authentication solutions.
- **Windows Azure Multi-Factor Authentication.** Another level of authentication in addition to a user's account credentials that satisfies compliance standards.

Retailers should consider more advanced methods beyond standard authentication, such as:

- **Callback.** Callback requires an authorized user to be in a predetermined physical location.
- **MAP/IP address check.** By restricting connections from IPs outside of an organization with an MIP/IP address check feature, POS devices can deny connections from remote users whose addresses do not appear on a predefined list.
- **Closed User Groups.** Retailers can receive custom serial numbers for the software used by service desk personnel and respective target devices. Only when the serial number of the service desk representative's machine matches that of the target device can a connection between the two be established. Other attempts will be automatically rejected.

If possible, choose a remote access solution that integrates with Active Directory and supports multi-factor options.

With access control measures in place and enforced, retailers should revise their official security policy and be flexible in making the necessary adjustments to bridge security gaps.

Physically protect your systems

Most retailers envision a physical breach as an attacker simply walking up to a POS terminal, inserting a USB drive and delivering malicious files into the network. But this is not the only scenario retailers must prepare for.



To physically secure a system, implement these three methods:

- **Control access to the system.** Make sure that all publically accessible systems are protected. To avoid physical malware infections, the USB ports of your systems should be disabled and card readers should only be placed in secure locations and bolted to counters. Further strengthen your access controls by enforcing the use of access control cards and biometric access control systems.
- **Implement surveillance measures.** Monitor the physical locations of your retail system using surveillance cameras and notification systems.
- **Periodically test your disaster recovery procedures.** Running disaster recovery drills can shed light on system weaknesses that may become entry points of an attack.



Consider contactless POS

Contactless POS systems leverage Near-Field Communication (NFC) while NFC-enabled devices allow customers to store credit card and loyalty information on their mobile phones. Moreover, customers can use their chip-and-PIN credit cards without the need for physical swiping through the POS terminal.

Monitor and maintain system integrity

1. Monitor privileged user activity

Monitoring privileged user activity on your critical systems is a security best practice as it allows you track unauthorized access into the retail system. Many regulatory standards such as PCI DSS explicitly require it.



2. Monitor system integrity

System integrity monitoring tools allow retail IT admins to save a snapshot of the system's configuration and then monitor any changes to files, registries, users, local and external groups, services, or rights policies resulting from software installations or unauthorized access.



3. Monitor audit trails & activity logs

Every digital interaction in a retail environment leaves a forensic residue. Extensive audit trails allow retailers to spot these clues to prevent and detect attacks. First and foremost, track and report on POS terminal activity in real-time and search for signs of unauthorized activity to identify threats.



4. Monitor authorized wireless access points

Requirement 11.11 of PCI DSS mandates maintaining an inventory of authorized wireless access points, including a documented business justification:



“The specific characteristics of each environment will dictate the appropriate methods or combination of methods to provide sufficient assurance that rogue wireless access points have not been introduced. For example, in the case of a single, standalone retail kiosk in a shopping mall, where all communication components are contained within tamper-resistant and tamper-evident casings, performing a detailed physical inspection of the kiosk itself may provide sufficient assurance that a rogue wireless access point has not been attached or installed into that kiosk. However, in an environment with multiple network nodes, it becomes more difficult to perform a detailed physical inspection due to the number of system components and network points where a rogue wireless device could be installed or hidden. In this case, it may be beneficial to combine one or more methods, such as performing physical system inspections in conjunction with the results of a wireless analyzer.”

– PCI Data Security Standard (PCI DSS), Information Supplement:
PCI DSS Wireless Guidelines, section 3.2.2 Physical and Logical Inspection

Most Importantly, Increase Security Awareness

The most important practice for stronger security in retail is security awareness.

Educate Your Staff and Increase Security Awareness

Security awareness throughout the complex retail infrastructure (including employees, third-party vendors, suppliers, merchants, and customers) reduces your chances of a breach and ensures an incident will be properly handled should it occur.

Formal security awareness programs for employees are mandated by many industry and regulatory compliance initiatives. PCI DSS requirement 12.6 mandates implementing *“a formal awareness program to make all personnel aware of the cardholder data security policy and procedures.”*

Developing effective security awareness

- **Create a strategy.** Your IT team will set up and support the security vision within your business, so involve them in developing a long-term strategy for training your employees. Along with this strategy, create a training plan and include key topics to address.
- **Be flexible.** Cyber threats are constantly evolving, so be flexible and open to updating the security training programs to cover the latest retail threats.
- **Establish timelines.** Train your employees in a timely manner to avoid a data breach. Educate them on current security best practices and the security policies in place at your business.
- **Test your employees' security awareness.** Send your employees fake phishing emails and simulate social engineering tactics. If someone within your organization falls into the trap, assign them additional security training. You might also consider sending out random security quizzes.
- **Offer incentives.** Consider adding incentives to your security training such as hours off, vouchers, or praising well-performing employees via internal announcements.

Conclusion

Defend the POS environment and customer data against the threat of sophisticated cyber-attacks by implementing multiple layers of security and enforcing security awareness across your entire network:

- Mandate P2PE, even for devices outside the scope of PCI DSS
- Segment your network and use firewalls to create a perimeter network
- Enforce a strong password policy and schedule regular software updates
- Manage detailed user rights and employ advanced authentication methods
- Physically secure your retail environment and monitor system integrity

Using these practices in conjunction will discourage potential attackers and mitigate the damage of a breach, but once again, it is most important to provide and promote security awareness to all staff. Remember, without security awareness in your organization there is no tool or security policy that can protect you.

Works Cited

PCI Data Security Standard (PCI DSS), Information Supplement (2011, August). PCI DSS Wireless Guidelines.

Section 3.2.2 Physical and Logical Inspection.

https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Wireless_Guidelines.pdf

PCI DSS Quick Reference Guide (2015, May). Requirement 8.6.

https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf

Payment Card Industry (PCI) Data Security Standard (2016, April). Requirements and Security Assessment Procedures. Version 3.2.

https://pcicompliance.stanford.edu/sites/default/files/pci_dss_v3-2.pdf

References

[Payment Card Industry \(PCI\) Data Security Standard](#)

[PCI P2PE Standard v2](#)

[Netop Remote Control Security Overview](#)

[Symantec Security Response: Typical anatomy of attacks against POS systems](#)

[IBM Research: Security trends in the retail security](#)

[Top Tips for Developing Effective Security Awareness](#)

[Social Engineering Attacks](#)

[Beyond the Point of Sale: Six Steps to Stronger Retail Security, SANS Institute](#)

[McAfee Solution Brief Security and PCI Compliance for Retail Point-of-Sale Systems](#)

[PCI DSS Wireless Guidelines](#)