WHITE PAPER

PREDATORS AT POINT OF SALE

Today's POS systems and PCI security standards provide a method for protecting stations from attack.

Executive Summary

Check the headlines on any given day. Chances are another large, multinational enterprise will probably have suffered a cybersecurity attack from one of today's well-trained and highly organized theft rings.

Retail and hospitality companies are among the industries most targeted by hacker attacks, according to Verizon's *2012 Data Breach Investigations Report*, an annual study of security incidents worldwide. Verizon says that point-of-sale (POS) servers and stations are primary targets for hackers because they often contain valuable customer information.

Most security breaches can be avoided if organizations follow best practices for information security. For example, Verizon recommends that merchants make two simple changes to their POS systems – changing default or easily guessable passwords and implementing a firewall – to prevent most attacks.

Given these trends, it's clear any organization that processes payment information must apply more stringent security measures to its POS systems. This is especially true given that POS systems have become the hub of many different enterprises, due to their tight integration with inventory, accounting, payroll and customer service platforms.

TWEET THIS!

Table of Contents

Today's POS Systems

These days, POS systems offer much more functionality than the electronic cash registers of yesteryear, which merely totaled receipts, calculated sales tax and dispensed change.

Today's IP-based POS systems feature speedy processors and easy-to-use touch-screen displays. They connect to a variety of peripherals, including barcode scanners, receipt printers and magnetic-stripe card readers. Increasingly, these devices perform complex transactions, such as processing coupons and redeeming gift cards, as well as handling sales, returns, exchanges and layaways.

While POS hardware is state of the art, it's the feature-rich POS software that makes these systems the central hub for running an enterprise, whether a retail business or any other organization that accepts payment for goods and services. The software gathers critical customer data that can be used to increase revenue or otherwise track an organization's ongoing relationship with the public.

Better Data Collection

POS systems have become data-collection and information-dissemination devices that enhance decision-making while allowing an organization to deliver better customer service. They gather detailed data about customers that is integrated with back-office operations. For example, managers may use such data to create targeted marketing programs, such as e-mail specials and real-time text alerts.

There are POS systems and software customized for various industries and vertical applications, such as restaurants, clothing stores, grocery stores, salons and gas stations. Salon POS systems not only handle payments but also track appointments and client rosters for reporting purposes.

At hotels, POS systems handle guest check-in and check-out as well as assigning dining room charges to guest rooms. And at hardware stores, for example, POS systems can support features such as special orders, repairs and rentals.

Although POS systems can be tailored to various industries, they all handle credit and debit card processing. And that's the information hackers want most. Therefore, increasingly, POS operators are turning to a set of security standards — called Payment Card Industry Data Security Standards (PCI DSS) — to reduce incidents of credit and debit card fraud.

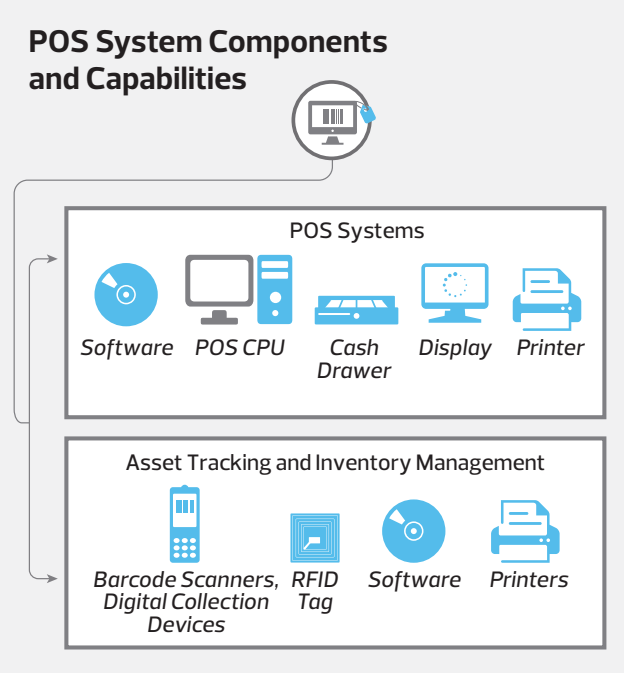
POS System Components

A POS system consists of several PC-based checkout stations that are linked via a computerized network to a main computer. POS systems provide significantly more functionality than electronic cash registers.

They can call up prices, calculate volume discounts, provide running totals of purchases and calculate sales tax. In addition, they can handle more complicated sales transactions, such as returns, exchanges, coupons, layaways, gift cards, rentals and loans.

A typical POS station comes in a rugged, all-in-one unit featuring a standard PC processor, Microsoft Windows software, an integrated hard drive, USB ports and a touch-screen display. Options include a magnetic-stripe reader, a customer display, cash drawer, receipt/thermal printer and barcode scanner. Keyboards, mice and battery adapters can also be added.

The newest trend is toward mobile POS systems that can support anywhere, anytime sales. Instead of having customers queue up for service, mobile devices allow employees to roam a store, for example, and serve customers in the aisles. Mobile POS devices include barcode scanners and magnetic-stripe readers to conduct sales, maintain inventory and handle payments — all in a compact, lightweight system.



Sophisticated Software

Through feature-rich software, POS systems record sales in real time, and keep inventory records and accounting systems current. By integrating with back-office systems, POS systems provide detailed data that organizations can use for stocking shelves and ordering merchandise. They also integrate with accounting systems to track cash flow and help prevent employee theft.

In retail, the reporting features of POS systems help managers gain control over their businesses. They can slice and dice real-time sales data and discover their best-selling products and most loyal customers. Managers can track sales and profits by time, day and seasons. And at the end of each day, they can determine inventory levels and cash positions.

The newest POS software integrates in-store and e-commerce sales, making it possible to create electronic newsletters and e-mail marketing campaigns and to send mobile alerts. E-commerce support is important for organizations that want to offer customers an online payment option they may not have had before, such as motor vehicle departments and school lunch programs.

When purchasing a POS system, organizations need to focus on the hardware-and-software combination that will allow them to provide the best possible customer experience. Another factor to consider is how well the POS software will integrate with existing back-office systems.

PCI Data Security Standard

One of the most important developments in POS systems is support for PCI DSS, which provides a framework for securely processing payment cards. Although its goal is to prevent data breaches, the standards help organizations detect and react to security incidents when they occur.

The standards were created and maintained by the Payment Card Industry's Security Standards Council, an open forum that was launched in 2006 to develop, manage and build awareness around security standards, including PCI DSS. The group's five founding members are the leading global payment brands: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa.

The industry group requires all organizations that accept credit cards to meet PCI DSS requirements. Failure to do so can result in penalties or sanctions from the members of the payment card industry.

PCI DSS is in version 2.0, which went into effect January 1, 2011. The PCI Security Standards Council maintains a website (pcisecuritystandards.org) with detailed documentation on how to comply with PCI DSS.

The PCI DSS includes 12 requirements that apply to businesses that process, transmit or store payment cardholder data. Merchants who follow PCI DSS must build and maintain a secure network for their POS systems, protect cardholder data, implement strong access-control measures and regularly monitor their networks for breaches. PCI DSS requires companies and other enterprises to analyze the IT systems they use for payment card processing, fix any vulnerabilities they find and conduct regular compliance reporting.

The PCI DSS reflects best practices for securing sensitive information. The standard requires purchasing various IT security systems and software, including firewalls, antivirus, access control, identity management and network monitoring.

PCI DSS requirements also include the encryption of cardholder data across open, public networks. There are encryption restrictions on primary account number (PAN) data as well as stored payment card data.

Selecting the right encryption algorithms and associated key management practices will simplify the implementation of PCI DSS. And clearly defining business needs prior to commissioning PCI compliance will also prove helpful.

PCI DSS and Small Merchants

Many small merchants are not in compliance. That's the conclusion of the Verizon *2012 Data Breach Investigations Report*.

While out of compliance with most PCI DSS requirements, these merchants are successful at encrypting transmission of cardholder data and sensitive information across public networks, and restricting physical access to cardholder data.

In contrast, the majority of large retail and hospitality organizations are meeting all PCI DSS requirements.

Levels of PCI Compliance

All merchants fall into one of four levels for PCI compliance based on their Visa transaction volume over a 12-month period. This includes all Visa transactions, including credit, debit and prepaid cards. The four levels are:

- **Level 1:** any merchant processing over 6 million Visa transactions per year
- **Level 2:** any merchant processing 1 million to 6 million Visa transactions per year
- **Level 3:** any merchant processing 20,000 to 1 million Visa transactions per year
- **Level 4:** any merchant processing less than 20,000 Visa transactions per year

Level 1 merchants must provide an annual report of PCI DSS compliance that is conducted by an external security expert or internal auditor. They also must have quarterly network scans for vulnerabilities and attest to their compliance with the standard's 12 requirements.

Level 2 and Level 3 merchants must complete annual self-assessment questionnaires on PCI DSS compliance, submit to quarterly network scans by a third party and attest to compliance with the standard.

Even the smallest merchants – operating at Level 4 – need to be PCI DSS–compliant. These small organizations must conduct self-assessments of their PCI DSS compliance, pass a third-party vulnerability scan, attest to compliance with the requirements and submit required documentation to their banks.

Complying with PCI DSS is not a one-time IT upgrade. Instead, it involves ongoing processes to ensure compliance.

Additional Security Issues

Remote access security becomes an issue when organizations install management software to diagnose, repair and patch

POS systems. These software packages open up a virtual back door into POS systems that hackers can exploit.

PCI DSS standards help to mitigate this security risk by ensuring the remote management software utilizes strong password protection, doesn't employ default settings and can be accessed only on a need-to-know basis.

POS systems typically include multiple stations connected to a single host system that serves as the central data repository and management hub. PCI DSS requires that host systems not store payment card information after transactions have been processed. Moreover, all access to host systems must be logged in accordance with PCI DSS, making it easier to find and stop breaches should they occur.

A final area of concern for POS systems is network security. Increasingly, POS systems use wireless networks for transactions and inventory control. PCI DSS rules ensure that wireless and wired networks are properly configured, have adequate security controls and log all network activity.

CDW: A POS Partner That Gets IT

At CDW, we offer a variety of POS systems with different levels of functionality and price points. Our vendors include Elo TouchSystems, Epson, Honeywell, HP POS, Motorola Enterprise Mobility, Pioneer POS and Zebra Technologies.

What's more, we can guide merchants through the process of determining what POS system, network, software and business processes are necessary for PCI DSS compliance – which may seem like a daunting challenge, especially to smaller organizations without dedicated IT staff.

CDW customers have a dedicated account manager, who serves as a single point of contact and a trusted resource. They can also tap the expertise of certified solution architects, who help integrate IT products and services from multiple vendors into a cohesive security solution. Our approach includes:

- An initial discovery session to understand your goals, requirements and budget
- An assessment review of your existing environment and definition of project requirements
- Detailed manufacturer evaluations, recommendations, future environment design and proof of concept
- Procurement, configuration and deployment of the final solution
- Telephone support as well as ongoing product lifecycle support

To learn more about CDW's POS solutions and PCI DSS compliance, contact your CDW account manager, call 800.800.4239 or visit CDW.com/pos-systems

Simplify your business and amplify your profits with an integrated system that helps you improve service and efficiency. Work worry-free with the solution that lets you focus on growing your business. The HP POS Solution, designed specifically to withstand the demands of the retail environment, is priced to fit within your budget. With industry-standard architecture, a small footprint and a retail-hardened design, it gives you the reliability and durability you expect from HP.

CDW.com/hp

Wasp Barcode Technologies offers a wide selection of barcode scanners, ranging from laser barcode scanners, wireless barcode scanners, 2D barcode scanners and CCD barcode scanners to point-of-sale barcode scanners. Wasp barcode scanners are easy to install and use, and feature flexible connectivity options including USB and Bluetooth™ wireless. Ideal for applications including retail, office, inventory, and manufacturing, Wasp barcode scanners offer the reliable performance a business demands.

CDW.com/wasp

The goal of store automation is to make checkout fast and easy for the cashier and the customer. Elo POS touchmonitors and touchcomputers are ideal in applications where cost, rugged design and flexibility are top criteria. Elo offers these products with an array of integrated peripherals. Elo also offers customization for large retailers. Elo products are designed for touch from the ground up, to ensure space-saving simplicity and clean and easy installation.

CDW.com

TWEET THIS!

CDW® PEOPLE WHO GET IT™