



[companies & products](#) [news](#) [research](#) [white papers](#) [classifieds](#)

[videos](#)

Search this Site: enter keywords

Go [Get Kiosk News in Your Inbox:](#) enter your e-mail address

Go [privacy policy](#)

WINCOR NIXDORF

Other Resources

- [Premium Reports](#)
- [Event Calendar](#)
- [Slide shows](#)

[printable version](#)

[email this article](#)



PCI, customer data and the kiosk

[Natasha Royer Coons](#), contributor
• 25 Mar 2009

If customer-data security was a big issue before, it became gargantuan in 2007, following the infamous TJX Companies security breach. More than 45 million customer records were compromised, causing the company to spend more than \$20 million investigating the breach, notifying customers and hiring lawyers for multiple lawsuits.

The crisis caught the attention of virtually everyone — from consumers, who heard numerous stories and warnings from multiple media, to retailers and other handlers of customer data. No longer could the need to protect financial information be treated as a secondary concern.

Enter the Payment Card Industry Data Security Standard,

Related Sites

Check out these sites for more news and information about self-service strategies and technologies:

- [Self-Service World](#)
- [Self-Service & Kiosk Association](#)
- [ATMmarketplace](#)
- [Digital Signage Today](#)
- [Retail Customer Experience](#)

Global Partners

- [ADFlow Networks](#)
- [Olea Inc.](#)
- [LG Electronics](#)

Get the latest kiosk news delivered to your in-box. [Click here to sign up for free.](#)

adeveloped by a council of multiple financial institutions to enhance payment-account data security. It includes guidelines for user authentication, firewalls, encryption, anti-virus measures and more.

Despite the increased focus, however, one path of credit card and other information from the consumer to the back office of the store and the bank has not seen enough attention: the kiosk.

Kiosk manufacturers and software developers in self-service should understand the importance of a secure kiosk network and how it affects their customers, and be prepared to introduce the right partners to help customers build, deploy and manage a robust kiosk network to meet the requirements of PCI DSS.

story continues below...



[Free Downloadable Special Publications](#)

[Digital Display Technology](#)

[Getting the Most Out of Your Kiosks](#)

[Self-Service in Grocery Stores and Supermarkets](#)

[Cash Automation Devices](#)

[Software Security](#)

[Cash Acceptance and Self-Service ROI](#)

[Kiosk Design](#)

[Interactive displays](#)

[Retail digital signage](#)

[Self-Service Branding](#)

ADVERTISE HERE

Reach thousands of potential customers through KioskMarketplace and its sister sites.

[Click](#) to find out how.

This story and all of our great free content is supported by:



[Convenient photo options in a snap.](#)

Frank Mayer & Associates, Inc. introduces the Sony® SnapLab® Pedestal. It is the perfect solution for mid-sized groceries, drug stores and convenience stores looking for a more compact photo kiosk solution. [For more information.](#)

Kiosk deployers and endusers should not only understand how to best secure their networks to comply with PCI DSS, but also assign someone on their teams, or even hire connectivity and security experts, to assume ultimate responsibility for securing the kiosk network and the customer data it captures and transmits.

The formation of the PCI council was announced in September 2006 and comprises American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. This article will look at a specific segment of PCI's complex body of rules and regulations and discuss the firewall and network components that are recommended to secure a kiosk network.

Relevant issues include protecting data at rest (storing information like credit cards) and in motion (sending credit card info for processing). Playing into that is whether the network is connected to the payment center or corporate headquarters by a wireless (cellular) or wired (DSL, cable) network, and what equipment and security setting is best for securing the data and protecting the network from intruders?

Firewalls

In the years of experience providing network expertise to the self-service industry, we at TeraNova have seen kiosk deployers utilize both software-based firewalls and hardware-

based firewalls in the kiosk to secure the data that is captured from the user. Here is some perspective on both:

Software. Many kiosk deployers utilize software-based firewalls to protect their networks from vulnerabilities because it's less costly. They simply use the server/processing unit inside the kiosk (often a computer with a Windows operating system) to ward off viruses, worms, trojans, bots, and other sorts of computer malware. They can block certain popular ports of entry such as port 80 and others. These deployers do not want to incur additional equipment or maintenance costs required to set up a separate firewall to launch a hardware-based VPN tunnel with encryption algorithms available to "scramble" the data in motion.

This relates directly to the TJX debacle. According to InformationWeek, poorly secured in-store computer kiosks were partly to blame for acting as gateways to the company's IT systems. The kiosks, located in many of TJX's retail stores, let people apply for jobs electronically, and they were connected directly to the company's network and servers. These kiosks were not protected by firewalls. An anonymous source said, "The people who started the breach opened up the back of those terminals and used USB drives to load software onto those terminals."

The source said the USB drives contained a utility program that let the intruder or intruders take control of these computer kiosks, essentially turning each kiosk into a remote terminal that could connect into the main network. The firewalls on TJX's main network weren't set to defend against malicious traffic coming from the kiosks.

According to Corey Nachreiner, senior network security analyst at WatchGuard Technologies Inc., a manufacturer of firewalls and other network security products, if someone is protecting a mobile computer, like a laptop used for business travel, then a software firewall combined with other security software might be "good enough."

If, however, someone is protecting a computer or network of computers that is not mobile, like a kiosk system, a hardware firewall often provides better protection.

Hardware. Software firewalls are designed to be just firewalls: they often can't block email or Web-based malware. "Malware" can be defined as software designed to infiltrate or damage a computer system without the owner's consent. If malware does infect a system with a software firewall, the malware can easily bypass that software firewall, or just simply turn it off.

In the past, many worms, trojans and bot clients were designed to actually add policies to various popular software firewalls, thus bypassing the software firewall and allowing malicious traffic to enter and exit the network at will. If the software firewall lives on the system (server/PC in the kiosk) and the malware infects the system, then the malware can easily reconfigure the firewall. If one has an external hardware firewall, even if malware does infect one of the internal systems, it can't make policy changes to that

firewall, since it's external to the system.

With kiosks, the security goal is often two-fold. The system needs to be protected from Internet and network threats, but also from the kiosk users as well. A kiosk is typically designed to only allow users to perform specific actions. Often, these types of kiosk systems implement security controls that try to prevent users from gaining unauthorized access to certain areas of the kiosks operating system.

Unfortunately, kiosk attackers have become experts at bypassing these restrictions and gaining unauthorized access to the operating system. If someone uses only a software firewall on the kiosk, and an attacker is able to bypass the local security restrictions, the attacker gains full control of that software firewall, and can disable it with ease. However, if a hardware firewall is used outside the kiosk, even if a local user gains access to the kiosk, he cannot disable the firewall.

In addition, software firewalls are sometimes ineffective at preventing attacks that target a system's operating system. Since a software firewall runs on *top* of an operating system, the operating system usually has to handle network traffic *before* the software firewall does. If certain components of that operating system suffer from security vulnerabilities, attackers could exploit them *before* the attack traffic actually reaches the software firewall. At that point, the hacker has already created a path to the kiosk processor.

Airborne attacks

Let's take another look at how the hackers got into the TJX Companies' network.

According to The Wall Street Journal, another separate entry point was an improperly secured Wi-Fi network the thieves accessed from the parking lot of a Marshall's store in St. Paul, Minn. The thieves reportedly used a wireless data-poaching tactic called "wardriving" and exploited the deficiencies of the aging Wired Equivalent Privacy (WEP) wireless security protocol. Although WEP is a security algorithm that can be enabled to secure the Wi-Fi network (802.11), it is susceptible to hacking.

Do not confuse Wi-Fi with cellular. Cellular refers to data that is transmitted directly between a device and a carrier's cell tower. Wi-Fi is the name of a popular wireless networking technology to provide high speed Internet and network connections in a wireless local area network (WLAN) using the 802.11 standards.

WEP a security protocol for Wi-Fi is based on a 64-bit or 128-bit shared key algorithm. WPA (Wi-Fi Protected Access) on the other hand, is an enhanced wireless encryption mechanism. But even WPA can have inherent weaknesses, although it is much more difficult to crack than WEP. The danger is that if an access point is hacked, the hackers can now sniff all the packets on the private Wi-Fi network.

There are a number of measures that can be applied with WPA to ensure higher barriers to hacking. For example, one can choose a long pass phrase over a simple password, and make sure it isn't composed of common words; a "brute force" dictionary program can run all common English words to uncover the pass phrase. If the hacker retrieves the pass phrase, they render the WPA security useless or at least highly vulnerable.

Builders of kiosk networks must be careful how they lock down their 802.11 security. Kiosk deployers may be leveraging a customer's Local Area Network (LAN) and using 802.11 (Wi-Fi) to broadcast that connectivity to the kiosks. Or they might bring in their own network but broadcast to multiple kiosks in the location. Either way, they need to secure the Wi-Fi portion of the LAN and the data as it is tunneled, encrypted, and transmitted across the Wide Area Network (WAN) to its destination, such as a payment processing center.

In fact, most security experts would not recommend the use of Wi-Fi unless there is a very specific and business critical reason to do so. If so, it's important that the wireless traffic be on a separate VLAN or network segment. Also be sure the WPA/WPA2 encryption and appropriate authentication as dictated by the PCI-DSS are enabled. In some cases, using Wi-Fi can add more PCI-compliance burden than it would cost to run DSL/cable or use a single cellular connection for each kiosk.

Point of capture

Jason Sweitzer, president of Tempus Technologies Inc., says, "Assessment of PCI compliance is a point in time."

Tempus Technologies is a technology vendor that focuses on point of sale applications, data warehousing, and payment processing for retail companies.

Indeed, PCI compliance is a moving target, and companies need experts and managed solutions to take the complexity and costs out of the ongoing exercise of maintaining security. Certifying costs are high, and if a deployer doesn't know what he is doing, not only is he in jeopardy of non-compliance and potential security breaches, but is spending more to process credit card payments. For a mistake in processing, the transactions can go from being charged at 1.5 percent to 3 percent from the merchant bank.

Here are some potential solutions for security at the point of capture as well as for protecting the data at rest.

- Sweitzer says Magnesafe technology, which encrypts track data on the head of the card reader, allows for the transmission of data without ever having unencrypted data on the kiosk network. This is one line of defense. Then the data should travel across an IPSec tunnel with at least Triple DES encryption to the data center. Again, this requires either a software-enabled tunnel and firewall or a standalone device that can launch the tunnel, encrypt the data and protect against intruders on

the network.

- File integrity management products can “protect” data at rest such as preventing it from being changed and providing alerts when the data is tampered with. This essentially ensures the “virgin” state of the kiosk so that the only programs that can run on the machines are the ones that have been loaded. Even if the kiosk network becomes compromised, the malware cannot run its programs.

How are other kiosk deployers handling the PCI compliance issues? Alex Doumani, vice president of engineering for Coinstar, says fraud and security are constant concerns, and they have invested heavily not only in PCI compliance but also in multiple layers of authentication and encryption for access and data transfer between the kiosks and the Coinstar data centers.

Smaller deployers of kiosks, however, need to watch the costs of deploying their networks and auditing for PCI, carefully weighing potential security risks and the need for more robust security options against doing the bare minimum for the network’s security. With the use of the proper network equipment, purchasing a few affordable managed services, and leveraging industry experts, those deployers will be able to offload the complexities of designing, deploying, and maintaining a secure network. For a reasonable cost, they can ensure they don’t fall behind on security requirements to protect their company and their customers’ assets.

Natasha Royer Coons is the managing director of TeraNova Consulting Group Inc. To submit a comment about this commentary, please e-mail [Tracy Kitten](#).

CLASSIFIEDS



[Easy Product Search Tool - "Rapid RFP"](#)



[Get RetailCustomerExperience magazine sent to you free!](#)

Related articles on this topic:



© 2009 NetWorld Alliance LLC. All rights reserved.