How to strengthen convenience store security

High traffic and employee turnover make the more than 150,000 convenience stores (C-stores) in the U.S. attractive targets for cyber-criminals. The nature of the C-store environment makes it difficult to deliver compliance and standardization. eMazzanti Technologies looks at what can business leaders do to strengthen convenience store security.

© iStock

Some brands in the retail space experience almost no turnover in staff. By comparison, convenience stores employ more transient workers. Deploying standards across all the stores proves difficult without having a regional or district manager visit every store on a regular basis. Hence, as studies show, C-stores and gas station chains tend to be the most susceptible to data breaches.

Criminals often use gas pump skimmers to steal payment card information. Since many gas station chains have yet to implement the EMV chip card technology for payment transactions, they suffer increasing card-stealing attacks. Fuel merchants face an October 2020 deadline (now April 2021) to

implement chip card readers at the pumps.

Evolving pump designs with flat payment terminals prevent the attachment of skimmers. However, bad actors now come in disguised as service techs to do a replacement or swap out.

They open the pump, and replace one terminal with a capture device, infecting the pump. No one questions them if they dress the part and no one catches the data theft until after the bad actors come back a few months later, remove the device and sell the data.

As happened recently at the Wawa and Rutter's chains, scammers also target merchant employees with phishing emails. If a worker clicks on an email link, it downloads malware that provides a back door for criminals into the network.

Delays in breach detection

Data breaches often elude detection for several months. This may be due to one or more of several possible reasons:

1. Sometimes the payment gateway provider fails to isolate the problem quickly.
2. Occasionally, the FBI decides not to let anyone know about an ongoing breach because they want to catch the perpetrators. Agents let the breach continue while they narrow down the suspects.
3. The perpetrators may let the device sit on the terminal for months before removing it to use the data for malicious activity.
4. Every so often, so many cards are stolen at once that the value of a card number drops very low and it takes a long time for the cards to be sold.

Cyber-criminals run a business. Revenue comes in from the sale of stolen data and they have expenses—what it costs to run a campaign, find people to buy the stolen data, and run servers. If their stolen inventory declines in value, they may hold on to it like an asset and sell it later.

How has COVID-19 impacted C-store data security?

We've noticed that municipalities, manufacturers and distributors—businesses deemed essential—are the ones being targeted now. C-stores are making money, they're open and they're essential.

They provide a quick and easy in-and-out for criminals. Mostly located next to major roads, bad actors get out of there quickly. Many lack working camera systems and basic security procedures. Hence, C-stores have become prime targets.

Some scammers also target merchant employees with phishing emails | © iStock

How to strengthen convenience store security

Since criminals look for the easiest targets, just being more difficult to attack than the next convenience store often deters them. Cameras posted on the ceiling—even if just the light is on—or an employee not doing the change on top of the cash register make the store less of a target.

A useful saying in retail goes, “eyes high and smile.” If you greet people when they walk in, they become less likely to steal from you. They know someone is paying attention and watching.

On the forecourt, you can seal the pumps. If the seal is broken, you know the payment terminal has been compromised. Only your vendor should have that seal. Someone can try to make that sticker, but why go through that trouble when they can go to the next C-store that does not use them?

C-stores have too much turnover to rely on training. It really comes down to policies and procedures. If people follow a procedure as part of their routine, then it shouldn’t matter who performs the job.

Also, when you select a vendor, use your contract to pass along responsibility for a breach to the supplier. That is typically enough to protect you. It is amazing how vigilant a supplier becomes if, in your terms of renewal, you pass along the liability.

Remember that the does should never be the checker. A mistake we have seen in convenience stores is that the same firm does both the security audit and deployment for an extended period. Thus, there are no fresh ideas coming in. The rotation of some of the vendors every few years is a good idea.

*Written by **eMazzanti Technologies**. The New Jersey firm provides IT consulting services for businesses ranging from home offices to multinational corporations throughout the New York metropolitan area, the United States and internationally.*