

February 15, 2019

8 Steps to Help Keep Your Payment Systems Safe

Payment management systems have a lot of moving parts, making their security a complicated process. Use compliance only as a starting point—you need to use best practices consistently to keep your systems secure.

Rodika Tollefson
Freelance writer and journalist



Despite chip-enabled payment cards, payment management systems remain a target for [cybercriminals](#). Lacking the resources of larger companies, small and medium-sized merchants are especially vulnerable.

In its [2018 Data Breach Investigations Report \(DBIR\)](#), Verizon found that small businesses comprised 58 percent of the victims of those data breaches where company size was known. (The DBIR analyzed more than 53,000 security incidents and 2,216 confirmed data breaches over a year, based on data contributed from 67 security vendors and government agencies globally.)

"Hackers have recognized that small businesses are low-hanging fruit because they don't have resources and the expertise," says Mike O'Malley, who works with small businesses as vice president of strategy for [Radware](#), a company that provides cybersecurity and application-delivery solutions.

The report found that payment data was compromised in the majority of breaches in retail (73 percent) and accommodations/food services (93 percent). Additionally, the top second and third assets involved in 2,023 confirmed data breaches were point-of-sale (POS) terminals and POS servers (databases were No. 1).

"For small businesses, it's a situation of survival because [...] when they have a [major] breach, the businesses don't survive," O'Malley says. "Small and medium businesses need to protect themselves with all the same tools as Tier 1 businesses, but the impacts for them are much more dramatic."

Being compliant with PCI DSS (Payment Card Industry Data Security Standards) is only the first step. To protect your payment management systems, you need to go beyond baseline compliance.

ADVERTISEMENT

Product Solution

Keep better tabs on cash flow

We help simplify money management. American Express has the solutions to keep you on top of your spending.

[Learn More](#)

1. Inventory your systems.

Begin by inventorying payment systems and processes, says Tommy McDowell, vice president of intelligence for the [Retail Cyber Intelligence Sharing Center \(R-CISC\)](#), a nonprofit information sharing and analysis center whose members range from "mom-and-pop" merchants to global retailers.

"You can't secure what you don't know you have," McDowell says.

He says an inventory is especially important when you have multiple stores, because there's always employee turnout and checkout counters get moved around.

2. Segment your network.

The multiple endpoints that are part of the payment management system put the network at risk, says Morey Haber, chief technology officer for [BeyondTrust](#), which provides privileged-access management solutions. Too often, he says, payment processing systems are on the same network as WiFi, Internet of Things devices and even guest WiFi log-in.

"Consider setting up a dedicated WiFi SSID (network name) for payment systems, or even use cellular payment devices to remove the risk of a shared network," he says.

Haber notes that while PCI DSS requires a complete inventory, mapping and diagram of the entire environment, "organizations typically fail to continuously discover, verify and prove these architectures are correct."

3. Train employees.

According to McDowell, bad actors often use targeted emails containing malware to locate payment systems and exploit vulnerabilities. The attackers can then gain foothold into the entire network.

"I'm consistently seeing scripts to exploit vulnerabilities in point-of-sale systems—especially in the firmware—for sale on the dark web," he says.

R-CISC has also seen an increased number of business email compromise phishing campaigns last year targeting retailers. A training program can help employees recognize phishing and other threats.

Sign up to receive the latest [business insights](#)

 [Join](#)

By providing your e-mail address, you agree to receive the business insights newsletter from American Express. For more information about how we protect your privacy, please read our [Privacy Statement](#).

"The first thing you need to focus on is education of your people, and teaching them about best practices and understanding how to best protect the business," O'Malley says.

4. Protect login credentials.

As a result of numerous major data breaches, more than 5.5 billion passwords have been compromised, according to [HaveIBeenPwned](#), a website that allows users to check whether their user names and passwords were part of data breaches. If you're reusing passwords to log into your payment management system or for remote access, you're giving bad actors easy access.

"Use two-factor authentication and have a long password that's very long to crack, and use a good password manager," recommends Scott Schober, president and CEO of [Berkeley Varitronics Systems, Inc.](#), which designs wireless and other threat-detection tools.

Schober also suggests anti-keylogger software and a dark-web monitoring service, both inexpensive. A monitoring service can check whether your personal information, including email and passwords, were exposed and when.

"It gives you an early warning," Schober says. "The sooner you're alerted, the better."

5. Implement change-management practices.

Because smaller businesses don't have mature security programs, they struggle with maintaining a consistent procedural approach and system monitoring, according to McDowell.

"You get an uptick in it, and then it swings away," he says. "And when it swings away, systems aren't patched as much as they should be."



Small and medium businesses need to protect themselves with all the same tools as Tier 1 businesses, but the impacts for them are much more dramatic.

—Mike O'Malley, vice president of strategy, Radware

You may also unknowingly disable a security feature after installing a system upgrade or patch.

"That's why it's very important to have a separate network to test when you do a patch and then rescan that device," he says. "You need good change-management practices."

6. Back up your data.

Multiple payment management systems—for example, several locations, phone sales, an e-commerce website and a third-party online merchant—create multiple points of failure. Schober says it's critical to have encrypted data backup, such as an encrypted, offsite backup system with PIN access.

"If you don't do that and at some point you're compromised, how do you go back to it and maintain business as usual when your customer database is in there," he says.

7. Use threat intelligence.

Nonprofit Information Sharing and Analysis Centers (ISACs) like R-CISC were established across different industries to help various sectors share information and best practices about threats and mitigation. McDowell says joining an ISAC keeps you proactive by giving you actionable threat intelligence.

R-CISC, for example, has a working group specifically for smaller members, and they benefit from data collected from the entire membership. McDowell says as a result of members' collaboration and data sharing and analysis, R-CISC has identified not only threats but also campaigns targeting specific equipment.

"When you have a small budget and talent pool, one of the best things you can do is join an information-sharing group," he says.

8. Outsource the expertise.

Whether it's using a [virtual chief information security officer](#) or a managed security services provider (MSSP), outsourcing allows you to focus on your core competency.

"If you're a small business owner, you have to be realistic [...] because the threats are too formidable, the [bad actors] are too sophisticated and the attacks are automated," O'Malley says. "To be on equal footing with them, take advantage of the managed service offerings."

When outsourcing, McDowell recommends asking the MSSP exact details about its security so you understand the gaps. For example, does the provider secure only the network layer, or the application layer too?

If you think you're too small to be an attractive target, O'Malley cautions that cybercriminals know large companies are very sophisticated and difficult to breach.

"Hackers know it's much easier to compromise a thousand small businesses, than one very well protected, instead of one heavily protected, big business," he says. "And many of the attacks are now automated, so they're much more effective because small businesses are not guarded at the same level as large ones."


Photo: Getty Images

Want to Dig Deeper?

- [Digital Tools](#)
- [Rodika Tollefson](#)
- [Getting Customers](#)



About the Author



Rodika Tollefson
Freelance writer and journalist