January 18, 2019

How to Help Protect Your Customers' Financial Information

The number of data breaches experienced by small and middle-market businesses is steadily growing, and compromised customers' financial information can especially put your company at risk. Fraud protection and data security require not only the right technology but also the right processes.

Rodika Tollefson
Freelance writer and journalist

Data-breach incidents can be devastating to small and middle-market businesses. When your customers' financial information is compromised, it's a strike against your company's reputation. Yet fraud protection and data-risk management are challenging if you're a small company with limited resources.

“Smaller businesses may think they're too small to be hacked, but they're the ideal target because they typically have less resources to mitigate attacks,” says Charles Keating, president of IT consulting firm Keating Consulting Service.

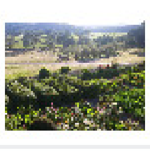
Cyberattacks on SMBs grew from 61 percent in 2017 to 67 percent in 2018, according to the 2018 State of Cybersecurity in Small & Medium Size Businesses report, an independent study conducted by Ponemon Institute LLC and sponsored by Keeper Security, Inc. (The report featured responses from 1,045 individuals from companies in the United States and the United Kingdom, ranging from less than 100 to 1,000 employees.)

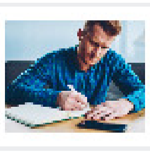
“Ultimately, small to medium businesses are just as exposed as large enterprises and will see the typical attacks that exploit human error and security weakness, as well as the same targeted attack methods as attackers move downstream,” says Carolyn Crandall, chief deception officer at Attivo Networks, which provides threat deception technology.

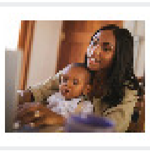
Customers' trust is often the largest currency that small and midsize businesses have, and reputational risk consequently incurs very high costs, says Ellison Anne Williams, CEO at Enveil, a startup providing data-in-use encryption.

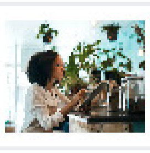
“Financial data represents your customers, and your customers put trust in your organization, so you need to ensure the data is secure in all parts of its lifecycle,” she says.

MORE IN GETTING CUSTOMERS

How 3 Businesses Successfully Adapted to Social Distancing


What Kind of Business Should I Start? How to Decide


How to Grab the Attention of Working Mothers


How Businesses Can Use Data and Customer Service to Adapt to Social...


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

Protect From Insider Threats

Tim Bandos, vice president of cybersecurity at data-loss-prevention company Digital Guardian, considers insiders the top threat. Whether they make accidental mistakes or act maliciously, being on the inside gives them easy access to valuable information.

Bandos says it's important to have a strong security culture, including an insider-threats program and security champions outside of the IT department.

“When you're trying to implement something, if it's coming out of the IT department, it can fall on deaf ears,” he says. “But if it's coming from the top, with the CEO or CFO promoting it, it can be just as effective.”

Keating believes that not investing into employee training is the biggest mistake that smaller businesses make. It's partly due to the high level of trust they place in employees.

“That level of trust leads to a false sense of security—businesses think they're safe inside their walls because they're a small company where everyone knows each other,” he says.

Mandatory security training should cover a variety of facets, from physical safeguards such as locking a computer workstation when not in use, to best practices against social engineering and phishing.

Encrypt Data Across the Lifecycle

Often times, businesses working hard to get ahead of the competition bypass critical steps like encrypting their data, says Dave Lewis, advisory chief information security officer with Duo Security, a trusted-access security company recently acquired by Cisco.

“People are often worried about how their data is handled in a cloud environment or another country,” he says. “If you encrypt your data, it doesn't matter where it resides.”

Williams says encryption is effective because it renders the data useless to attackers. For example, if they steal credit card or other financial information, they receive garbled bits instead of a string of numbers they can repurpose.

Sign up to receive the latest business insights

Enter your email address

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.

“If they break in and take the encrypted data, they can't do anything meaningful to it—they can't exploit it,” she says. “[Encryption] also has the effect of greatly deterring attackers from breaking in because if you're encrypting at every step of the lifecycle… they can't do anything with it and their motivation goes way down to attack the organization.”

She notes, however, that the focus is typically on data at rest (where it resides, like a database) and in transit (transmitted through the network), but not when it's in use. So when the information is decrypted in memory—for example, to conduct analytics on customer transactions—it's still at risk.

“If I'm an attacker, I can patiently wait until you go use your data, and steal it when it's decrypted in memory—so everything you've worked hard to protect… is now exposed,” she says.

Manage User Access

While encryption is becoming standard practice, Williams says it needs to be used with other control mechanisms, such as user access controls.

By limiting the number of people who can access the financial data of your customers, you're limiting your exposure. Additionally to managing access to sensitive data, best practices include strong passwords and multifactor authentication.

> “
>
> That level of trust leads to a false sense of security—businesses think they're safe inside their walls because they're a small company where everyone knows each other.
>
> *—Charles Keating, president, Keating Consulting Service*

“If you've used the same password in several places, it's time to let that go and have unique passwords,” Keating says. “And it's time to use a password manager to manage those passwords because you're not going to remember them.”

Reused or stolen passwords could be used to attack your company's website as well, and Bandos says websites are “the perfect gateway for cybercriminals.”

“They can easily 'knock on the door' and drop directly into the network, or they can spend hours on the website to scrape customer information,” he says.

Adoption of multifactor authentication is on the rise, but Lewis of Duo Security cautions that not all those authentication methods are created equal. Email and SMS are some of the more common methods of multifactor authentication, yet they're also more susceptible to intercepting. He recommends a method such as WebAuthn (using asymmetric cryptology), which is supported by the World Wide Web Consortium (WC3).

“Even if an attacker is able to access a database of static passwords, they can't gain access to the system because they don't have this other method of authentication,” he says.

Prepare for the Inevitable

Crandall says that small and medium businesses can be victims of the same type of attacks as large companies, but without the security controls and staff to address them.

“Common mistakes that smaller companies make are typically around underestimating their attractiveness as a target, lacking detection security controls and not understanding how prepared they are to respond,” she says.

An incident response plan is critical for knowing what to do postbreach, according to Bandos.

“An incident response plan can help you to quickly contain a breach so it's not a knee-jerk reaction,” he says. “It can help limit your data exposure.”

Photo: Getty Images

Want to Dig Deeper?

Rodika Tollefson Digital Tools Getting Customers

About the Author

Rodika Tollefson
Freelance writer and journalist