Restaurant Cyber Crime
How to defend your business
April 2020
Build Your Cyber Defense

The threat from cyber crime today should put us all on alert. Cybercriminals have a goal: breaking into businesses like yours to prey on your employees, compromise your data, and ultimately tap into your—and your customers’—accounts.

The hospitality industry has emerged as a prime target for cybercriminals. New technologies that improve restaurant operations and enhance customer service are here to stay, but the potential opportunities they create for cybercriminals and the risks they pose—in the back office and at point of purchase—are real and constantly evolving.

At Bank of America, we are committed to helping our clients understand the importance of defending against cyber crime. We want restaurant operators to recognize the risks and to take precautions to protect their businesses and their customers.

We understand what’s at stake. Cyber breaches and data theft not only threaten your reputation and your customer counts, but also can leave you exposed to long-term damages.

A first step in cyber crime prevention is education. That means prioritizing employee training, participating in industry conferences and investing in technologies that can counter criminals’ efforts.

We’re here to help. Our team has an ear to the ground; we share what we learn, both from others in your area and from clients around the world, in materials like this. We also use our knowledge and experiences to offer ideas that can help you protect your organization, and help you combat cyber crime before it occurs.
But today’s growing cyber crime threats are more ominous, and potentially much more costly. A restaurant might be the target of a criminal, who sends a phishing email in search of access to the company treasury. Or the attack might come from a thief using a skimming device to steal credit-card information, or a criminal infiltrating a restaurant’s databases through its POS system or vendor connections.

“Regardless whether it is a sole operator, franchisee, or franchisor, cyber security should be just as important as food quality, and should be ongoing and discussed by management as frequently as anything else connected to the business,” says Charles Murphy, senior treasury sales officer, Bank of America.

The numbers on cyber crime are staggering and startling. The FBI estimates that businesses have lost more than $12.5 billion to email crime over the past five years.¹ Cybercriminals are busy. In 2017 alone, they perpetrated data breaches that exposed more than three billion personal information records, six billion email accounts and more than two billion Facebook accounts.² Data breaches are increasingly costly—in terms of investigation and recovery costs, reimbursement to customers whose credit cards are compromised, and crisis communications costs, as well as lost business.
On average, a data breach costs an organization $7.35 million, according to the 2017 Ponemon Institute Cost of a Data Breach Study, including $4 million in lost revenue from wary customers who take their business elsewhere.⁠¹⁰

The foodservice industry has a set of characteristics that make stores vulnerable to theft of all kinds, but especially losses due to cyber crime — including a large volume of transactions, high employee turnover, a wide-ranging network of both local and national vendors, and extensive digital connections to corporate and regional offices as well as IT and POS providers.

As more quick-service restaurants and chains have responded to changing customer habits, like allowing customers to pay by credit or debit card via a mobile device, their response has opened up new vulnerabilities in front-of-the-house systems. And while the use of payments has expanded, the restaurant industry has been slower than others to adopt the payment industry’s protective chip or EMV technology; chip readers are an expensive investment, and some think they slow down the transaction.

Cristin O’Hara, Restaurant Group managing director and group head, Bank of America, says, “Restaurant industry executives understand they need to change their approach. All this technology is here to stay, and with it, the security risks are only getting larger. Cyber security is an investment to protect their business and their reputation.”

Mary Rosendahl, director of Global Digital Channels, Fraud Education and Risk Management for Bank of America Global Transaction Services, points out that many of the biggest and most expensive cyber attacks still start with a simple email that hits an unwitting target. One click on an attachment, or a reply to a fraudulent email address, can open the door to these criminals.

Different phishing emails have different goals, but the primary objective is to get access inside an organization. For example, a company might receive an email message from a purported “vendor.” The message indicates the vendor is updating or changing its bank account and asks the restaurant to change the information in its payment system. Looking closely, there usually are clear signs of deceit, such as an inaccurate email address or phone number.

But if an employee doesn’t catch those mistakes, and changes the vendor information in the system, payments can be sent to criminals’ bank accounts. The organization suffers a double loss; not only is the money lost, but the actual vendor still needs to be paid.

“A huge amount of fraud is still perpetrated through phishing emails,” Rosendahl says. “Someone sends an email, and manages to get login credentials and passwords when an employee mistakenly clicks on a link or changes information in the restaurant company’s system. That allows the criminal to start looking in the company’s system for information.”

Email fraud losses over five years

$12.5 billion

¹¹Ponemon Institute 2017
²²017 data, Cybersecurity Ventures
Once inside a company’s network, cybercriminals also might try to install malware—software designed to damage or disable a system—onto an organization’s computer network, sometimes demanding a ransom in order to restore the system and its data to normal operations.

Finally, criminals will attempt to break into an organization’s database of information—either through the POS system or back-of-the-house servers—to steal the personal or financial information of customers and employees. Once harvested, the data is sold to other criminals.

These data breaches have the potential for the most widespread damage. “First off, there is a huge risk to your brand reputation with customers; we’ve seen that in other large data breaches,” says Murphy. “But I’m not sure every company knows the risks and liabilities connected with a breach if it happens through the POS system. An operator may think the POS provider would pick up the costs associated with a breach—but ultimately at the end of the day it’s the restaurant operator who will absorb all the costs.”

The cost of a data breach, on average, is $225 for each credit card or customer record that is exposed, according to the 2017 Ponemon study, that includes everything from the cost of forensics investigations to fines to replacing customer credit cards. And a restaurant or chain’s database might include thousands or even millions of customer records.

“This isn’t limited to the restaurant industry,” Rosendahl says. “Every single data breach that is occurring today is related to some sort of credential compromise, often via a phishing attempt and often through a back door, like a third party’s connection to a computer system.”

Some experts say restaurant companies need to take a hard look at cyber security—now. “As criminals’ attention on other industries has diminished, we have seen the restaurant industry, as well as hotel food and beverage, become a prime target over the last six to eight months,” says Larry Brennan, senior vice president, Merchant Data Security and Cybersecurity director for Bank of America Merchant Services.

Brennan says cybercriminals recently have zeroed in on restaurants’ connections to vendors of POS systems and general IT support. “The main cause of these breaches are credential compromises,” he says. “The criminals open a back door into the POS system, and then can deploy malware to the server, get to all the franchises and gather customers’ credit-card information.”

Murphy and Rosendahl remind chain executives that it only takes one vulnerable spot to open up the entire network to criminals. “When you’re in the restaurant business and have franchises, you may be secure at the corporate level. But all you need is one franchisee who has chosen not to invest in securing his systems,” Murphy says. “If that franchisee gets breached, and that allows a criminal access to all your stores and corporate systems, what does it mean for your company and your brand?

“If I’m a franchise owner and another franchisee gets breached, it doesn’t just hurt them—it hurts all of us, our entire brand.”

225 dollars per credit card or customer record is the average data-breach cost
“If I’m a franchise owner and another franchisee gets breached, it doesn’t just hurt them— it hurts all of us, our entire brand.”

Charles Murphy
Senior Treasury Sales Officer
Bank of America
Front-of-the-house vulnerabilities

1 Credit & debit cards
The industry’s accelerated move toward non-cash payments — credit and debit cards — has created new opportunities for criminals, as POS connections and terminals have become a key access point. “In many ways, restaurant operators can look at this trend as a positive, because with it, the industry is not only making customers happy, but also moving away from the risk of in-store theft; employees are not handling money as much,” says Bank of America Restaurant Group head Cristin O’Hara. “But on the flip side, the use of credit card machines opens more restaurants up to the threat of a data breach. It’s that much more critical to invest in the right safeguards to avoid data breaches.”

2 POS terminals
New and ever-more-sophisticated skimming devices are targeting your POS systems to steal your credit card information. And these aren’t your father’s skimming devices. These days they can be Bluetooth-enabled or 3D-printed skimmers that can sit on top of or overlay a regular point-of-sale terminal. “It used to be that a bad actor would give a restaurant employee a skimming device, and then pay that employee to use it to skim and steal credit-card numbers,” says Brennan. “You don’t see that as often now, partly because of video camera technology and identification systems that make employees too recognizable. But these new skimming devices allow cybercriminals to sidestep the employees to get what they want.”

3 Vendor systems
One of the newer and growing threats comes via integrators and resellers — the tech companies that install and support a retailer’s payment systems. These vendors’ systems can be used by criminals as a back door into a restaurant’s own systems. Here’s one way it works: Typically POS vendors use simple usernames and passwords when establishing a client account; often it’s the same default username and password for all the vendor’s new accounts. If individual stores or offices don’t take the time to change those usernames and passwords, a determined criminal will look for a restaurant still using those default IDs, and gain entry to the store’s POS system — and possibly more of its computer databases. Brennan says that right now, as much as 40% of data compromises for retail establishments are related in some fashion to these connections with a reseller.
4 Chip reader technology
Although it can represent a significant investment, chip reader technology can help prevent some POS crime. In their fourth year of deployment, credit card machines equipped to read microchipped cards have dramatically cut the use of counterfeit credit cards at the point of purchase. They don’t help, obviously, when a customer is ordering offsite or online. Says O’Hara, “Not everyone has switched to chip technology. Although clearly worthwhile, it’s a huge undertaking for any restaurant company. But the investment in chip reader technology can stop fraud at the register.” Some restaurants have gone a step further and installed chip-and-PIN card readers, which require customers also to provide a PIN number to complete the transaction, and represent an even more secure option.

Back-of-the-house vulnerabilities

1 Remote access
There is no way around it; the business world’s use of technology expands the number of possible places a criminal can target. Says Brennan, “When you look at how the restaurant industry operates, a store now depends on remote access to upgrade menus, to run its POS system and to connect into the corporate environment. Those types of connectivity, and each of those connection points, expose you to criminals and to malware.”

2 Business email compromise
Despite all the high-tech tools used to infiltrate a computer network, a huge amount of cyber crime still occurs through business email compromise (BEC). BEC is a tactic used by criminals to attack all sorts of businesses, including foodservice operations. Cybercriminals typically target back-of-the-house employees and computer servers, using different tactics to gain access to server data. They might send phishing attempts via email, with the goal of accessing data or installing malware. Says Brennan, “Ninety-nine percent of breaches are caused by human nature. It’s someone clicking on a link, or changing information in the vendor system so that a criminal has access to the store’s information.”

3 False invoices
Because restaurants rely on an expansive network of vendors, both national and regional suppliers as well as local vendors, there are a variety of access points for criminals. And although some are digital connections between restaurants and vendors, some fraud occurs much more simply. O’Hara points out that even the franchisee of a national quick-service restaurant chain can use a surprisingly large number of paper checks to pay local businesses responsible for things like landscaping and maintenance. O’Hara says, “Watch for people creating false invoices for services that didn’t happen. It’s easy for some of these things to go under the radar — like a window cleaner making up a false invoice, or for a false company.” O’Hara suggests a best practice: Establish two-factor identification for anyone writing checks, and have two employees sign every check. She also recommends using a bank’s payee positive pay service, which matches the checks a company issues with those being presented for payment. “It’s a first rung of crime protection,” she says.

4 Payroll fraud
New technology allowing employees to deposit a payroll check via a bank’s mobile app has created problems for some restaurant companies. “One type of crime we’re seeing more frequently is employees who are paid by check trying to deposit that check twice — once through a mobile banking app, the other with the actual paper check in person at a bank branch,” O’Hara says. “It’s an opportunity somewhat like check kiting.” Murphy suggests this: “A company should put a policy in place to let employees know that if they attempt this sort of double deposit — whether they’re being nefarious or just uninformed — the company can prosecute them,” he says.
Despite an increased use of credit and debit cards, and experiments with cashless restaurants, says Charles Murphy at Bank of America, "The cash side of the business should never be overlooked."

Bank of America Restaurant Group head Cristin O’Hara knows that store owners and managers worry all the time about the possibility of an armed robbery. "They’re worried about people’s safety, whether it’s a robber in the store attempting to bust open a safe, or someone targeting the store manager when he’s taking the deposit bag to the bank at the end of the week," says O’Hara.

Like many restaurant and banking industry experts, O’Hara is a proponent of smart safes, which are being added rapidly throughout the retail industry. A smart safe is typically small enough to fit under a quick service restaurant’s front counter, near the cash registers or in a back office. Employees deposit cash directly into the safe, entering a PIN number, an employee ID number, the amount of the deposit and register receipts, or information. If the information all matches — if the actual cash matches the deposit information — the safe accepts the deposit. Once a week or more frequently, an armored car stops by the store to safely transport the cash to the bank.

Murphy says the benefits are obvious: Smart safes eliminate the need to physically take the money to the bank, reducing the risk of an employee being targeted and robbed en route to the bank branch. "It also removes the finger pointing that can occur between a manager, an employee and the bank if a deposit doesn’t match the store’s records," he says. "The safe can capture the cash from each register, and speed up the collection process."

Although like cyber security measures, smart safes require a serious capital investment. Murphy says the more smart safes are deployed by restaurants, the more executives should consider making the investment. "You don’t want to be the last store on the block taking cash," he says. "You don’t want to be the one that criminals target."
What can you do to help protect your restaurant or your chain against cyber crime? Experts offer these suggestions to reduce your risk of being impacted by a cyber event.

**Conduct IT audits**
Conduct a complete audit of your store or chain’s back-of-the-house IT systems and front-of-the-house POS terminals and applications. Make sure all software is up to date and patches are installed. Carefully examine how your systems are connected to other stores, to corporate headquarters and to individual vendors’ systems. Murphy says, “We tell a company they should identify all their systems — software and hardware — and how those systems are connected both to the internal network of their business and to external systems. Understand what information is being transmitted from system to system, and ask: Does that information serve a purpose? If not, find a way to shut it down.”

**Safeguard your data**
Protect your data with point-to-point or end-to-end encryption, which keeps data safe while it travels from computer to computer — from your store to corporate headquarters, for instance — preventing criminals from accessing data as it’s being transferred.

**Restrict computer access**
Limit access, and especially remote access, to your computer systems and servers. Murphy recommends an informal audit, asking who has access to systems, both employees and external vendors and consultants — and then asking the follow-up question: Should they have access?

**Vet your vendors**
Use Certified and Qualified POS integrators and resellers to install, manage and support the POS system; ensure that their applications are installed properly, and that remote access to the POS system is not simply left “always on.” Make sure that any passwords your store uses to access systems are not easy-to-guess default passwords. Visit the Payment Card Industry Data Security Standards Council website (pcisecuritystandards.org) to check the list of qualified and certified vendors. Note that Visa requires many of its merchants to use Certified and Qualified Integrators and Resellers. Implement a policy of two-factor authentication for everything, from writing checks to accessing the store systems from remote locations.

**Install chip readers**
If you don’t have them, consider investing in chip readers at the point of sale. Visa has found that for merchants who have installed chip-reader technology, fraudsters’ ability to use and steal credit card numbers has dropped dramatically; in a 2017 report, Visa said counterfeit-card fraud has dropped by two-thirds for chip-enabled merchants.

**Police your POS**
Conduct a daily check of your POS terminals and credit-card readers to make sure nothing has been tampered with. Look for possible skimming devices installed on POS devices. Devices located in quiet or unattended areas of a store can be vulnerable, but so can devices in high-traffic areas where employees are multitasking and might not be able to continually monitor machines. Use special tamper-resistant screws, cable locks and stickers or other identifying markings to make it easy to see if a device has been compromised.

**Encourage risk awareness**
Raise awareness among your employees, particularly the back-of-the-house team in accounting, payroll and corporate management, about the dangers of phishing emails. Encourage everyone with access to your system to use best practices by choosing secure passwords and changing them on a regular basis.

**Watch for trends**
Finally, stay informed. “Because it’s a fluid situation, and because criminals are always one step ahead of law enforcement, someone at every company should be actively participating in conferences and webinars, talking to peers, and collaborating on this issue with banking and financial partners like Bank of America,” says Murphy. “Going to industry trade shows is also a way to be in the know about the latest trends.”
Neither Bank of America nor its affiliates provide information security or information technology (IT) consulting services. This material is provided "as is," with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this material, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, quality and fitness for a particular purpose. This material should be regarded as general information on information security and IT considerations and is not intended to provide specific information security or IT advice nor is it any substitute for your own independent investigations. If you have questions regarding your particular IT system or information security concerns, please contact your IT or information security advisor. No information contained herein alters any existing contractual obligations between Bank of America and its clients.

"Bank of America" and "BofA Securities" are the marketing names used by the Global Banking and Global Markets divisions of Bank of America Corporation. Lending, other commercial banking activities, and trading in certain financial instruments are performed globally by banking affiliates of Bank of America Corporation, including Bank of America, N.A., Member FDIC. Trading in securities and financial instruments, and strategic advisory, and other investment banking activities, are performed globally by investment banking affiliates of Bank of America Corporation ("Investment Banking Affiliates"), including, in the United States, BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp., both of which are registered broker-dealers and Members of SIPC, and, in other jurisdictions, by locally registered entities. BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp. are registered as futures commission merchants with the CFTC and are members of the NFA.

Investment products offered by Investment Banking Affiliates: Are Not FDIC Insured • May Lose Value • Are Not Bank Guaranteed.

©2021 Bank of America Corporation. All rights reserved. 3485014 01-21-2383