Cybersecurity 101

A TOOLKIT FOR RESTAURANT OPERATORS

entréeNet

Are you prepared?

The digital age is transforming the way restaurants do business. Innovations in technology have only just begun to help restaurateurs streamline operations, reduce their costs, and bring more guests into their restaurants.

With opportunity comes risk. Innovation in the restaurant business—whether in payments, marketing, operations or even menu analysis—depends on processing large amounts of data, more than we can imagine. It's this data that criminal hackers are profiting from.

It seems like every day there is a new data breach. The Target breach at the end of 2013 was an early, wide-scale breach, exposing the payment card data of millions of customers. However, the threat is now evolving. As we have seen in multliple other breaches, cyber criminals are now looking for information other than payment card data—details about employees, confidential company financials, and corporate secrets.

In times like these, protecting payment card data—while still very important—only goes part of the way.

Think about your own operation. You have more than just card data at stake. Through mobile applications, loyalty programs and social media, you may be collecting guest data such as age, address, favorite orders, and visit frequency. You likely track your food, beverage and labor costs, as well as your suppliers' pricing. Your systems hold intellectual property like new recipes and business endeavors. You store employee and payroll information, data on customer interactions, social media trends, and maybe even data on your competitors.

ALL OF THIS DATA IS VULNERABLE.

We know that cybersecurity isn't why you got into the restaurant business, but it's emerging as one of the biggest risk factors for your reputation and your bottom line. The threat is growing, so you need to take steps now to protect your business.

Hackers know that you face time and resource constraints. They prey on businesses that are ill-prepared for an attack. That's why an ounce of prevention is worth a pound of cure. Just as you have made food safety an integral part of your quality assurance program, you need to also make cybersecurity a part of your operation. Improving security is a lot less expensive than dealing with a data breach.

In this paper, we lay the foundation for you to take those first steps. You will learn about the five aspects of a fully formed cybersecurity program. You will need to dive deeper into many of these topics, but this high-level guide gives you a solid framework to move forward.

Why Cybersecurity Matters

Five ways a data breach can hurt your restaurant company

The costs associated with a data breach can be overwhelming. Payment card breaches, for example, can easily add up to $100,000 or more in losses, fines and forensic audits—an expense many restaurants cannot survive. Those are just the financial costs. It's hard to predict how much brand damage you might experience if data you've collected on your customers or confidential internal information is compromised by hackers.

Let's look a little more closely at five key ways a data breach could cost your restaurant business.

1. INVESTIGATIONS, FINES AND REMEDIATION

If a breach involves payment card data, you'll face substantial fines from the card brands since you will have violated the card acceptance agreements that require you to remain compliant with the Payment Card Industry (PCI) Data Security Standards.

To see just how costly these fines can be, Transaction Resources Inc. added up all of the fees and penalties merchants must pay when their payment card information has been stolen. Fees and penalties include forensic investigation fees, security remediation, card brand compromise fees, card reissuing and monitoring fees, and fraud-reimbursement penalties (chargebacks).

Just the suspicion of a data breach of customer payment cards requires a forensic audit by an approved PCI forensic investigator. Based on the size, complexity and extent of the breach, forensic fees can range from $12,000 to more than $100,000 per investigation.

Vulnerabilities uncovered by the forensic investigation must then be remediated. Transaction Resources says updating your security may require hardware, software and network modifications at an average cost of over $2,000.

Even a suspected data breach can be costly

Scott Carlson, owner of Court Avenue Restaurant & Brewing Company in Des Moines, Iowa, knows firsthand the jarring impact even a suspected data breach can have on a restaurant.

In his case, there wasn't even a breach—only the suspicion of a breach. But that was enough to trigger a series of costly actions that have become all too familiar to operators and merchants victimized by cybercrime.

Carlson was notified by local authorities of suspicious activity on some of his patrons' credit cards. A common point was that all had dined at his restaurant. Even though no card fraud was ever linked to his establishment and no suspicious activity has occurred since, Carlson says Court Avenue incurred significant fines and losses from the incident.

"Restaurants have become the victims," Carlson warns. "They are bearing huge costs, even if it is only a suspected breach."

"Unequal burden of responsibility"

The impact of just one suspected breach, Carlson says, carries "an unequal burden of responsibility." He adds, "The POS companies, processors, banks and credit card networks don't pay any fines. We're the ones that get hit." Among the consequences that he suffered and says other operators need to be aware of:

- Processors will request detailed compliance information, requiring you to cross-reference each potential breach with your employees' work schedules.
- Processors and card networks can require you to conduct a forensic audit, which can cost thousands of dollars—and must be conducted by one of only a handful of approved vendors.
- If the card network suspects there has been a breach, it can fine you thousands of dollars for allegedly violating the networks' data security rules, even if no actual fraud losses can be proved.
- Worst case, the credit card company can refuse to accept further transactions.

Carlson says that restaurateurs have no choice regarding the fines. He was charged $6,000 by MasterCard and Visa even though there has never been any evidence that a breach occurred at his restaurant. In other words, an operator can do everything possible to prevent fraud, as he did, and still get stung.

What's the answer? Even though Carlson had just invested in a new POS system that was PCI compliant, he decided he needed to take further steps to protect his restaurant, including upgrading computer hardware and tightening controls on access to his systems.

With the help of a resourceful part-time IT person, Court Avenue was able to isolate and restrict the IP addresses that are allowed access to its POS system. According to Carlson, "Now we know exactly who is accessing our systems and why."

Other precautions taken by independent operators like Carlson have included building stronger firewalls to protect networks, installing security cameras to monitor POS systems, training employees on data security, and limiting access to company computers.

In addition, each card brand assesses fines for the merchant data that is compromised. Transaction Resources says that these fees typically start around $5,000 and can exceed $500,000, depending on the size of the breach. Chargebacks can also add up since stolen cards may remain in circulation long after the breach.

Altogether, Transaction Resources estimates that the average small business pays $36,000 to $50,000 for a data breach.

2. 47 DIFFERENT STATE BREACH-NOTIFICATION LAWS

Businesses that have been breached face increasingly complex notification rules. As of early 2016, 47 states have laws on security breach notification, according to the National Conference of State Legislatures.

These laws detail when a company is responsible for informing its customers or users in the event of a breach. All the laws are slightly different, which makes compliance difficult for multi-state operators.

Provisions of these laws explain who's covered, what type of compromised personal information will trigger notification requirements (e.g., account numbers, name combined with social security number, driver's license or state ID), what constitutes a breach, requirements for notice once a breach has occurred and exemptions (such as for encrypted information).

Many restaurateurs and foodservice operators simply collect name and payment card information from their guests, and nothing more (no email or mailing address). When this is the case, and you don't have any other means of informing your customers, almost every state law will require that you provide "substitute notice" by informing statewide media that you've had a breach.

That's right, you must inflict further damage on your reputation by informing the media that you've been hacked. This has the effect of harming your brand well beyond your core customers.

Increasingly, states are going beyond security breach notification laws. More states are getting prescriptive about the steps businesses should take to secure their data. The outcome could be a patchwork of state-level regulation that makes compliance even more difficult.

3. INEVITABLE CLASS-ACTION LAWSUITS

To make matters worse, it's the notice to your guests or the media that whets the appetite of trial lawyers. Your notice may trigger tort lawsuits for failure to protect, inadequate security and negligence. Class-action litigation costs can add up quickly.

A recent decision by a federal appeals court against Neiman Marcus clears the way for lawsuits after a breach, even if no fraud or harm has occurred. Customers may be able to sue simply based on the risk they face following a breach.

Breached companies also have been the target of regulatory action by the Federal Trade Commission. The FTC is using its so-called Section V authority, which bans unfair and deceptive trade practices, to go after companies that it says put consumers' personal data in danger. A recent appellate court decision affirmed FTC's work in this area, even though the agency has no written rules or guidelines about what constitutes "reasonable" cybersecurity.

4. INESCAPABLE BRAND DAMAGE

It's difficult to quantify how much your restaurant's brand will suffer if a data breach is found. For businesses that suffer a breach, one of the biggest challenges is holding on to customers.

Research by the Ponemon Institute reveals that reputation and the loss of customer loyalty do the most damage to the bottom line after a breach. "In the aftermath of a breach, companies find they must spend heavily to regain their brand image and acquire new customers," according to Ponemon's 2014 study on the cost of data breaches.

In a separate survey of more than 800 executives in 2011, Ponemon found that an organization's brand value dropped between 17 percent and 31 percent following a breach and that companies spent up to a year restoring their reputation.

The polled executives estimated their company's brand value to be anywhere from $1 million to greater than $10 billion, with an average of $1.5 billion. Depending on the type of information stolen, companies, on average, lost between $184 million to more than $330 million in the value of their brand, according to the survey.

5. LOOMING CONGRESSIONAL ACTION

Policymakers are intent on addressing the problem of data breaches through complex federal and state laws and regulations. The pressure to find a solution builds with each new breach. The National Restaurant Association has been advocating for one federal data breach notification law, but banks and financial institutions have been active on Capitol Hill demanding that Congress impose stringent new data security standards on merchants. They allege that merchants are irresponsible data custodians and need more direct government regulation.

Congress has not yet agreed on an approach, but as the battles in Washington heat up, restaurateurs need to stay involved to counter the threat of lopsided solutions.

5 Essential Steps to Protect Your Business

Given all the threats, it makes sense to take a proactive approach to cybersecurity. Before we get started on how to do that, you should know that cybersecurity is fundamentally an exercise in risk management. You won't ever be able to remove the risk entirely, but you can take steps to mitigate it. Risk is not anything new for restaurant operators. You took a big risk just opening your restaurant. You learned to reduce the risk of failure and improve your rate of success by following certain procedures and instilling in your team an attitude for success. You can do the same with cybersecurity.

THE FIVE FUNCTIONS

Stakeholders from all sectors of the economy recently came together to create a framework that businesses of all types can use to identify cyber threats and protect their establishments against data breaches. This framework, launched in 2014, is formally known as the National Institute for Standards and Technology's (NIST) Cybersecurity Framework for Critical Infrastructure. It's a long name for something very simple. At its core are five functions: **Identify, Protect, Detect, Respond** and **Recover**. A focus on these five can help you create a cybersecurity blueprint for your restaurant.

While it's not a panacea, having a plan that addresses each of these five functions can go a long way toward protecting your restaurant. And the good news is that this framework works well for all sizes and types of restaurants—from small establishments just starting to think about cybersecurity to the most sophisticated operations and franchised companies.

Once you've operationalized these five functions, you will have taken that important next step towards protecting your business against cyberattacks and possible data breaches.

Is the NIST framework required?

It's best not to think of the five functions of the NIST framework as a to-do list or a requirement for compliance. In fact, beware of vendors who try to sell you "NIST compliance." It's a guide and a way of thinking—not a mandate.

The beauty and simplicity of the framework is that it can be adapted and scaled to any restaurant configuration: a single operator, a multi-unit operator, a franchisor, a franchisee.

For an independent restaurant operator, you can use it within your four walls. For a franchisor, it can be a way to educate your franchisees about your cybersecurity programs and track their progress. For a multi-unit restaurant operator, it can become a shared operational guide for your IT staff, store managers, executives and board, so that members of your team are all speaking the same language.

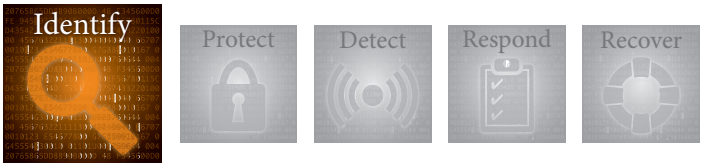
According to NIST, "The framework will help an organization to better understand, manage and reduce its cybersecurity risks. It will assist in determining which activities are most important to assure critical operations and service delivery. In turn, that will help to prioritize investments and maximize the impact of each dollar spent on cybersecurity."

YOU'RE NEVER FINISHED ...

As you examine the components of the NIST framework, keep in mind that it's a process. Think for a moment about quality assurance. Your QA programs are designed to ensure consistent food preparation and good service. QA is an ongoing process. Can you honestly say that you are ever done with QA? By the same token, cybersecurity is not about checking boxes, although there are certainly checklists you can and should use to protect against threats. Rather, cybersecurity is a continual process that you need to build into your daily operations. Threats will change, but if your cybersecurity program is designed properly, you'll be able to respond accordingly and adopt new policies to reduce the risk of cyberattacks.

Remember, there are no shortcuts. You may be tempted to focus more time and energy on the first two steps—**Identify** and **Protect**. These surely are important, but you also need to be equally concerned about **Detect**, **Respond** and **Recover**.

1 Identify



WHAT ASSETS ARE AT RISK?

Your first step is to take an inventory of all of your systems and **Identify** just how much risk you face. You need to know what you have before you can protect it. Ask yourself these questions:

- What systems or hardware—like point-of-sale terminals—connect to your network, and what kind of information do they collect? What software do they run?
- Do you operate a website, a mobile site and/or a mobile ordering site?
- How are you connected to the Internet? Do you have a firewall in place?
- Do you allow your employees to access your network remotely?
- Where do you store the information you collect? How does it get there? Is it through an automated system or over a wireless system? How long do you keep the data?
- What is your most sensitive data? Where is it stored?
- Who has access to your data (including third parties like your credit card processor, loyalty program administer or part-time IT consultant)?
- Who on your staff is responsible for cybersecurity and compliance activities? How are decisions on these issues made?

Answering these questions helps identify your risks and vulnerabilities, whether it's a piece of equipment or a source of data. The **Identify** function helps you to determine how much risk you have.

Restaurants and other merchants are attractive targets for hackers because they process so many card transactions. But those aren't the only vulnerabilities you have. As you consider your data risks, you will undoubtedly uncover other types of sensitive information that your restaurant holds.

Beyond payment card information, you may be collecting back-office information like restaurant financials and food costs, employee data (including social security numbers) and supplier information. The growth of mobile and loyalty programs in the restaurant industry brings risks. If you're collecting customer data through a mobile option or third-party application, be sure to identify it.

Where do you store the information you collect? How does it get there? Is it through an automated system or over a wireless system? How long do you keep the data?

2 Protect

TAKE STEPS TO STOP A CYBERATTACK BEFORE IT BEGINS

Once you've identified your cybersecurity risks, you can turn your attention to protecting your data to stop a cyberattack before it begins. In the **Protect** step, we'll look at tactics and procedures you can put in place to strategically leverage your resources and protect your restaurant.

The key aspects of the **Protect** function include:

- Limiting access to information, data sources and equipment like servers, either through explicit policies or passwords.
- Training staff on your cybersecurity procedures and policies.
- Determining if your employees tasked with cybersecurity and compliance responsibilities have adequate and appropriate training.
- Ensuring that your systems are updated with new security updates or patches from the developer or manufacturer.
- Implementing steps to protect your most sensitive data. This includes such compliance activities as meeting PCI standards, as well as other steps, like making sure passwords are changed at regular intervals.

No one-size-fits-all solution

There are no one-size-fits-all solutions to cybersecurity. Every business is unique. You have different point-of-sale systems, different operations, different processes and different pieces of information beyond the payment card data you may retain. To be effective, the tactics and tools you employ must be tailored to your operation, taking into account your tolerance for risk and your available resources.

Follow best practices

While there isn't a single solution, we know that the vast majority of targeted cyber-intrusions could be prevented by incorporating these simple, best-practice mitigation strategies: limiting access, training staff, ensuring your systems are updated and protecting your data.

▶ **Limiting access:** Armed with your answers from the **Identify** section, you should now be able to determine who has access to your equipment and data sources. By limiting who can interact with your restaurant's computer server, for example, you can prevent a rogue or careless employee from inadvertently downloading hostile or intrusive software, including computer viruses and other malicious programs.

Access controls apply not only to in-person interactions but to remote ones as well. Many point-of-sale systems allow individuals to view the receipts for the day from a remote site. Since this activity occurs off premises, operators must be vigilant about adopting and enforcing controls on who can view such data. Several restaurants in Delaware recently experienced data breaches due to failure to protect this functionality. Hackers may find smaller restaurant operations more

attractive because these businesses often allow users to access data remotely and tend to lack full-time IT support.

Recall that even Target, one of the largest retailers in the United States, was hacked because its remote portal for vendors was vulnerable to attack. Cyber thieves were able to use login credentials from an air-conditioning contractor to penetrate Target's internal systems. The lesson is that you can never have too many controls when it comes to remote access.

▶ **Training staff:** Educating your employees about who can access your equipment is an important aspect of cybersecurity training. Employees should be informed about who has responsibility over these matters, and who can give authorization for internal access as well as access to service technicians and other third-party vendors like processors.

If there is turnover in a position that has cybersecurity responsibility, be sure to update your employee information and change passwords or codes once the person leaves the position. If you don't, those employees or former employees will be able to access your information.

▶ **Staying up to date:** As part of your **Identify** efforts, you inventoried not only the hardware or equipment you use in your operation but the software, too. In addition to protecting the data your software collects, you must make sure you are running the most up-to-date version of your software. Software developers constantly discover new vulnerabilities in their software's code and will forward patches to fix those problems. Hackers take advantage of companies that haven't patched their systems. Be sure you have systems in place that ensure you are patching all of your software at regular intervals.

▶ **Protecting data:** Too often, critical computer systems are left unprotected and easily hacked because of the failure to change the password that came preloaded on the system. Hackers know and exploit this vulnerability with the greatest of ease. As a starting point in your efforts to **Protect** your data, you should outline procedures that ensure that passwords across your enterprise are changed at regular intervals, and especially after employee or vendor turnover.

When it comes protecting payment card data, the starting point for any restaurant is compliance with PCI standards. All merchants that process, store, or transmit cardholder data from American Express, Discover, JCB, MasterCard and Visa International must comply with these standards. As discussed earlier,

EMV is only part of the solution

Given that most of the cyberattacks in the restaurant industry occur at the point of sale, you might think the new EMV or chip cards are the perfect solution. These new cards use a microcomputer chip to generate a dynamic card value that is nearly impossible to counterfeit.

Unfortunately, there has been a lot of misinformation about EMV. The truth is EMV will not protect restaurants from data breaches. At best, EMV provides an added layer of security. It will stop the use of counterfeit credit cards in your establishment, but frankly that's a type of fraud that doesn't happen very often in restaurants.

The EMV "liability shift" that took place in October 2015 simply means that merchants without EMV- or chip-enabled terminals now face liability when card-present fraud occurs. Merchants face no regulatory or legal requirement to install EMV card readers. It is a business decision that each company must make.

If you have not yet converted your systems to EMV, you might take a look at what you pay in chargebacks due to counterfeit cards. If it's not a lot, your dollars might be better spent on other data security protections such as tokenization or encryption.

The PCI Security Standards Council has warned that even with EMV, credit card numbers remain unencrypted during transactions. The largest breaches of card data in the United States have come from vulnerabilities within the merchant or processor environments that EMV does not address. This is why a focus on enterprise-wide cybersecurity and the five core functions of the NIST framework is so necessary.

Chip + PIN: Is the United States headed in that direction?

It's still up in the air whether chip + PIN, a security feature used with EMV cards in Europe and Canada, will catch on in the United States.

At least for now, EMV cards are being implemented in the United States with chip technology only. By contrast, EMV cards in Europe and Canada are issued as chip + PIN and require a PIN to be used at the point of sale instead of a signature. The chip + PIN approach gives merchants a second layer of authentication.

President Obama threw his support behind chip + PIN for the United States in 2014 when he signed an Executive Order requiring the federal government to use chip + PIN technology for government-issued cards and accept these cards at federal facilities such as national parks. He also called on private industry to adopt EMV and use chip + PIN.

The technology continues to raise questions, and it's possible that more dynamic technologies like mobile payments will eventually supplant the need for PINs generally. In the meantime, if chip + PIN security gains ground in the United States, restaurateurs will need to figure out whether the extra layer of security is worth the added cost of an extra piece of equipment— specifically a PIN pad—for use at tableside and at drive-thrus. The National Restaurant Association is watching this issue closely and will keep its members updated.

failure to do so will result in steep fines from the card brands, even if your operation is merely accused of a breach.

It's not enough to be PCI compliant. PCI standards are aimed only at protecting payment card data, so PCI compliance is only part of the security game. Look at all the systems you inventoried in the **Identify** function, then make sure you are taking steps to protect each of these data sources.

PCI leaders themselves are aware of the system's limitations. Stephen Orfei, general manager of the PCI Security Standards Council, noted in a presentation at the 2015 NRA Show that the PCI Data Security Standard is "moving away from a compliance orientation to a risk-based approach." Rather than look at PCI compliance as a once-a-year audit process, Orfei said foodservice operators need to adopt an ongoing risk-based strategy, which is the same approach NIST recommends in its five-function cybersecurity framework.

Protecting data through encryption and tokenization

As payment and other technologies evolve, so do cybersecurity tactics. Restaurateurs and foodservice operators need to keep pace.

On the payment card side, EMV cards (see page 6) are certainly more secure than magnetic-stripe cards, but EMV cannot prevent fraudsters from stealing unencrypted data. Once data from a sales transaction hits the Internet, there is a strong likelihood that hackers can capture it—unless the information is encrypted and stays encrypted all the way to its destination.

End-to-end encryption has thus become a primary goal for both merchants and processors when it comes to protecting card data. Several companion data-protection technologies look promising as well, among them tokenization, which shields sensitive consumer information by substituting other data that cannot be used by thieves.

"With data security, the best defense is a good offense," says Michael English, vice president of product development for Heartland Payment Systems. "By taking the card data out of the transaction—and out of a merchant's ecosystem—you remove the ability of hackers to get anything of value. You cannot monetize encrypted card data."

English suggests that the most secure way restaurants can go is to combine end-to-end encryption with EMV capability and tokenization. EMV cards help reduce counterfeit-related fraud, but the biggest vulnerabilities in the payments process are often not about fraud. They're about where a card is swiped or the card number is entered, where the card information is stored, and how the card information is transmitted. Restaurateurs need a game plan in each area.

Encryption converts plain-text information captured at the point of sale into cipher text that requires a key to decrypt. Tokenization returns a token to the merchant in the authorization process instead of a credit card number. Tokens replace sensitive data with random, unique numbers that have no value to thieves. The token can also be used for returns, recurring payments, sales reports, etc.

Tokens can also be used as a substitute for the primary account number (PAN) you may be using to identify customers for your loyalty programs and other customer promotions. When you use tokens, thieves who steal your data come up empty-handed.

The PCI Council's Stephen Orfei agrees that EMV, end-to-end encryption and tokenization "are the three technologies that will get us to the endgame. They will protect your business and will devalue the data, so that it's useless in the hands of organized crime."

The power of encryption doesn't end with payment card data. You can apply encryption to all of the data your restaurant collects and that you've inventoried as part of your **Identify** efforts.

3 Detect

ROUTINE MONITORING CAN HELP YOU PICK UP A PROBLEM

Once you've **Identified** which assets are at risk and taken steps to **Protect** them, you'll need to put systems in place to **Detect** whether you've been breached.

Just as it's necessary to have smoke detectors, fire alarms and fire extinguishers in your restaurant facility, it's imperative that you have the tools to quickly detect a breach and promptly take action before the "fire" gets out of hand. By monitoring and detecting a problem ahead of time, you will put yourself in a far better position if a breach does occur.

It's less costly to take steps now than to wait until the authorities or your processor notify you there's been fraudulent activity associated with your restaurant.

There are a number of detection systems you can put into place. Consider implementing systems such as the use of a web-log analysis tool and processes that allow you to set a baseline of what normal or "unbreached" systems look like, for example.

Checking your systems at regular intervals can lead to detection of abnormal activity. For example, you should check to see if any large files are being transferred out of your POS system, perhaps customer credit card numbers kept on file in case of a chargeback investigation. Other signs of suspicious activity include unexpected Internet and network traffic, unknown files, software and devices installed on your systems, disabled antivirus programs, increased after-hours activity on your systems, and unknown applications that launch automatically when you reboot.

Simply having a routine detection procedure can reduce the likelihood of a longer, bigger and more expensive data breach.

REDUCING DETECTION TIME

Unfortunately, the hospitality industry has not been quick to detect cyberattacks. Verizon's 2015 Data Breach Investigations Report found that in 78 percent of cases in the hospitality sector, incidents took months or longer to discover. Compare that to the average across industries, where 74 percent of incidents were discovered within hours.

Verizon suggests one reason for the delay in discovery is that restaurants are likely to be notified of an incident by an external party, such as a fraud alert, rather than internally.

Remember, the longer an attack goes unnoticed, the longer criminals have access to your systems and operations. As a result, the potential for data theft and loss of information is significant.

4 Respond

PLAN FOR THE WORST, AND BE READY TO ACT

Respond is how you react in case a breach is discovered—either through your own detection efforts or through contact with the authorities or your payment processor. Once you've been breached, time is of the essence! While you've worked hard to **Protect** yourself by aligning your resources with your risks, you must also be ready to respond in a worst-case scenario. This will save you time, money and stress, and mitigate further damage to your restaurant.

WHAT YOU NEED TO KNOW

To respond to a data breach, you will need to work with IT professionals—in-house and external, as appropriate—to round up answers to the following questions, just as a start:

- What data was compromised or stolen?
- How did you find out about the breach?
- How did the breach occur? When and where did it happen?
- If the breach is still happening, how can it be stopped? If it's over, how long did it go on?
- Who was affected by the breach? Guests? Employees? Suppliers?
- What are the legal requirements? Beyond the law, do your contracts set any legal obligations in the event of a breach?
- Does the law require you to inform guests about the breach? The media? Both? What will you say? Are you prepared to issue a press release?
- Do you have lawyers you can consult who know about cybercrime? Who else would you need to call? Do you have their phone/cell phone numbers?

Take time now to prepare a data breach response plan. This is a detailed blueprint that spells out how your operation will respond if a data breach is detected through your efforts or discovered by an outside party. Putting together a plan is not a one-time task. You will need to review your response plan at regular intervals to ensure you have the most up-to-date information.

Your answers to the above questions will set the stage for your next steps. Some post-breach responses are dictated by the law. As noted earlier, most states have data breach notification laws. Familiarize yourself with your state's notification requirements. Federal laws and regulations may also be relevant, including the Federal Trade Commission's enforcement authority.

Other response requirements may be spelled out in contracts or agreements with third parties. If the compromise involves payment card data, your card brand will have specific guidelines for you to follow. For example, you may be asked not to turn off, access or alter the compromised systems. You should preserve all logs, document all actions you

Putting together a plan is not a one-time task. You will need to review your response plan at regular intervals to ensure you have the most up-to-date information.

take and alert appropriate incident-response personnel, including your merchant bank and law enforcement.

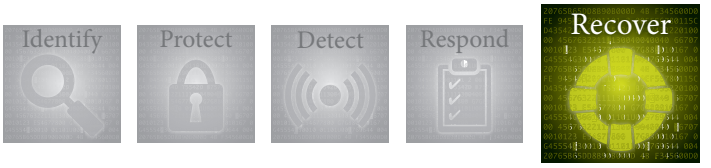
Simply having the cell phone numbers and emails of key people to contact can save precious time if a breach is detected. Your first call after detecting a breach should be to a lawyer who is well versed in cyber-crime. After that, all activity should be run through the attorney. Your communications with your attorney or law firm will be protected by attorney-client privilege, and these experts will be able to work with you to mitigate the impact of potential lawsuits.

Ask the right questions of your third-party vendors

That loyalty card company that you use—what if it has a breach of your customers' data? What happens then?

You should make it part of your due diligence to find out how third parties protect your guests' personal information and be sure to review their processes throughout the life of your contract. Be sure to ask them about their security and privacy policies, and talk through what happens if there's a breach. It's certainly possible for you to seek indemnification for the costs and liability of a breach as you negotiate your contract with them.

5 Recover



GETTING BACK TO NORMAL AFTER A BREACH

Much like the **Respond** function, **Recover** entails planning. Again, the purpose is to save precious time in the event of a breach. If your restaurant is taken down by a breach, how will you get back to normal? This function also calls for learning—what lessons can you apply to your operations to avoid future breaches?

Think about the steps that you will need to take to earn back the trust of your customers. That alone will likely strengthen your resolve to improve your cybersecurity procedures and pay more attention to the first four functions of the framework.

You need to consider, too, the financial resources it will take to recover. As we noted earlier, data breaches are expensive. It may be worth considering cyber liability insurance so that you have an extra layer of financial protection.

As we've noted, recovering from a breach can be a lengthy process. Here are some questions you should be prepared to answer:

- Have you fulfilled all of your legal obligations, including notifying law enforcement and your guests (via state newspapers, if required)?
- Are you prepared for a slowdown in business? Look for ways to trim expenses and increase your promotions.
- Are you prepared to deal with employee terminations? If business slows, you may have to lay off employees, or you may need to take action against an employee who was negligent or violated your data security policy.
- Have you considered hiring a public relations firm to help you rebuild your reputation?
- Have you changed your passwords, and updated your software and hardware? (See **Protect**.)
- Have you considered hiring an IT expert to conduct a security audit to prevent future incidents?