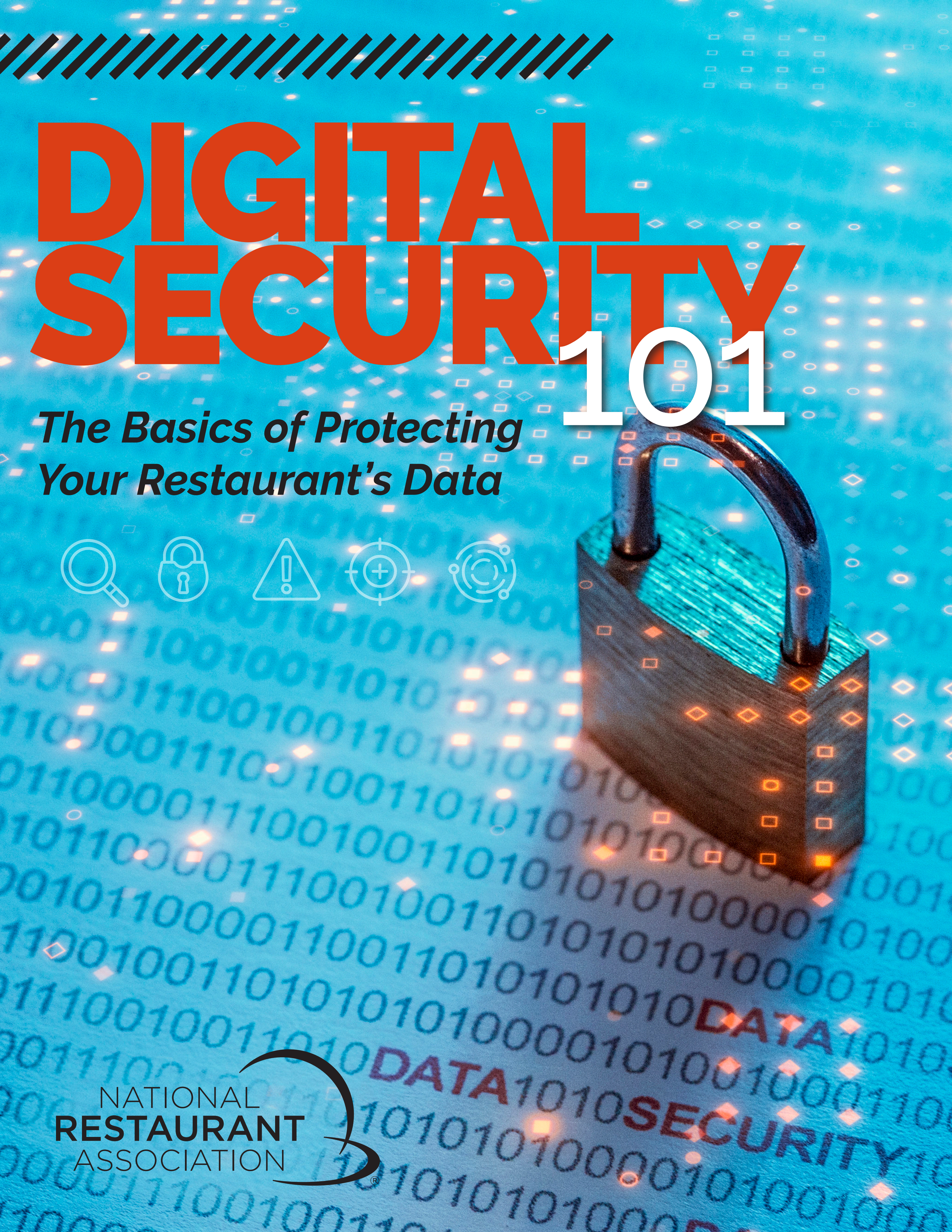
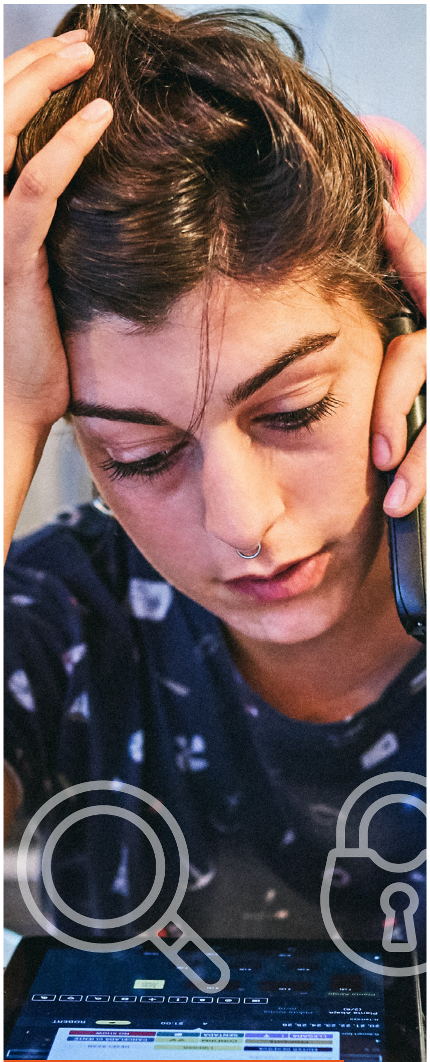
DIGITAL SECURITY 101

The Basics of Protecting Your Restaurant's Data



NATIONAL RESTAURANT ASSOCIATION®



AN INDEPENDENT RESTAURANT OWNER GETS A CALL:

someone has been **stealing credit card numbers from her customers**, charging more than $100,000 in the last three months. Her processor bank says **she must submit to an expensive forensic audit**, and she faces thousands of dollars in fines from the card companies.

THE CEO OF A QUICK-SERVICE RESTAURANT COMPANY LEARNS

that **hackers have grabbed his customers' information**, including their names, addresses, contact information, social media handles and buying history from the vendor handling the company's loyalty program. Now **he'll have to hire a law firm that specializes in these breaches**, and notify customers about the breach, based on individual state breach-notification laws.

A CASUAL DINING CHAIN'S MARKETING MANAGER CLICKS

an email asking his company to participate in "Restaurant Week," **unwittingly launching a cyberattack on the company**. An on-screen message says that all proprietary information has been seized and will only be released after the **company pays a bitcoin ransom**.

SIMPLE ACTIONS TO HELP YOU PROTECT YOUR DATA

A little planning will go a long way to protect you from data theft.

The digital age is transforming the way restaurants do business. Tech innovations streamline and automate restaurant operations and most of those innovations are fueled by data.

And whenever data is handled — card payments, payroll and human resources records, inventory control, or loyalty programs — **online criminals and hackers are lurking, waiting to attack where restaurants are most vulnerable**.

Think about your own operation. You have more than just card data at stake. Through mobile apps, loyalty programs and social media, you could be collecting guest data such as age, address, purchase preferences, and visit frequency.

Back of house, you track your food, beverage and labor costs, as well as your suppliers' pricing. Your systems hold intellectual property such as new or proprietary recipes and business plans. You store employee and payroll information, data on customer interactions, maybe even data on your competitors.

Even during the coronavirus pandemic, hackers never sleep. If anything, your business is more fragile and vulnerable now than ever before, and some types of digital attacks are on the increase, according to the Center for Internet Security.

Phishing, ransomware, "denial of service" attacks and malware are only a few of the ways cyber thieves attempt to steal valuable data.

The good news is you can take steps to protect your operation and your customers so you're less susceptible to data breaches and other cybercriminal activity.

Preventive measures can make a huge difference.

Security matters

*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.*

WHAT YOU CAN DO

The National Institute for Standards and Technology developed the Cybersecurity Framework for Critical Infrastructure. The Association has adapted the NIST framework for the restaurant industry. At its core are five functions:

- **Identify**
- **Protect**
- **Detect**
- **Respond** *and*
- **Recover**

Using these five functions as a foundation, you can build a data security plan for your operation that will go a long way toward protecting your business.

Think of the NIST framework like a Hazard Analysis Critical Control Point (HACCP) plan for digital safety. By carefully building a plan that fits your unique situation, you'll be better positioned to avoid data security threats to your restaurant.

Each of the next five parts of this resource will focus on one of the NIST framework functions and give you an overview of how you can easily begin to develop your own data security plan.

HERE ARE FIVE WAYS A DATA BREACH COULD COST YOUR RESTAURANT

✔ **FINES, INVESTIGATIONS, AND REMEDIATION.** If a breach involves payment-card data, you'll face substantial fines from the card brands. Why? Because all card acceptance agreements require you to remain compliant with the Payment Card Industry Data Security Standards. Breaches cost the average small business between $36,000 and $50,000. Fines alone for major breaches can far exceed $500,000.

✔ **STATE BREACH-NOTIFICATION LAWS.** Each state has its own law governing how you must notify customers of a data breach. All the laws are slightly different, which can make compliance difficult for multi-state operators. The Association has lobbied Congress to enact a single federal statute, but Congress has yet to act.

✔ **CLASS-ACTION LAWSUITS.** Breach notification typically triggers class action suits, and customers may be able to sue simply based on the risk they face following a breach. Even a suspected breach can trigger legal actions and negative press. Costs can add up quickly.

✔ **BRAND DAMAGE.** Damage to your reputation and the loss of customer loyalty can severely impact your bottom line after a breach.

✔ **POTENTIAL CONGRESSIONAL ACTION.** Despite the Association's advocacy, banks and financial institutions allege that merchants are irresponsible data custodians and need more direct government regulation.

IDENTIFY

The first step in the NIST Cybersecurity Framework is identifying which of your restaurants' digital assets are at risk.

Allowing data thieves or malicious actors access to your networks and computer systems can damage your reputation and end up costing you tens of thousands of dollars in fines, fees and remediation. You can lose customers, revenue and even your business.

The first step in building a plan to prevent any loss is to **Identify** the risks you face. Take an inventory of all your systems and networks. You need to know what you have before you can protect it.

ANSWER THESE QUESTIONS:

□ **What systems or hardware** — such as 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 app?

□ **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?** Consider third parties like your credit-card processors, loyalty program administers or part-time IT consultant.

□ **Who on your staff is responsible for data security 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 for hackers because they process so many card transactions. But those aren't the only vulnerabilities you have.

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, identify it.

PROTECT

Once you've identified which of your digital assets are at risk, use these steps to plan how to protect them.

Taking an inventory of your systems and networks helps you identify how much risk you face. In this ***Protect*** *step, we'll look at some quick ways you can substantially reduce your vulnerability.*

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 retain.

To be effective, the tactics and tools you employ must be tailored to your operation, considering your tolerance for risk and your available resources.

While there isn't a single solution, we know that most targeted cyber-intrusions could be prevented by incorporating the simple, best-practice mitigation strategies cited below.

FIVE KEY STEPS

✔ **LIMIT ACCESS:** You should know who has access to your equipment and data sources. By limiting who can use or log into 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.

Controlling access applies to remote interactions as well. Many POS systems allow individuals to view the day's receipts from a remote site. Operators have to be vigilant about controlling who can view such data.

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.

✔ **TRAIN STAFF:** Employees should be informed about who's responsible for your systems, and who can give authorization for internal access as well as access to service technicians and other third-party vendors such as distributors.

Update your employee information and change passwords or codes if there's turnover in a position that has data security responsibility. You don't want former employees to have access to information.

✔ **DOWNLOAD PATCHES:** Protect the data your software collects by making sure you're running the most up-to-date version of your software. Hackers also take advantage of companies that haven't patched their systems. Put systems in place to ensure you're downloading patches for all your software regularly.

✔ **CHANGE PASSWORDS:** One of the most common ways hackers get into computers is due to weak passwords or passwords that came preloaded on the system. Protect your data by changing passwords regularly too, especially after employee or vendor turnover.

✔ **PROTECT PAYMENT CARD DATA:** Comply with Payment Card Industry Security Standards Council (PCI SSC) standards. All merchants that process, store, or transmit cardholder data from American Express, Discover, JCB, MasterCard and Visa International must comply with these standards.

If you don't, you might face steep fines from the card brands, even if your operation is merely accused of a breach. You can find out how well you're adhering to the standards by taking PCI SSC's Self-Assessment Quiz.

Look at all the systems you inventoried in the ***Identify*** *function, then make sure you're taking steps to protect each of these data sources.*

DETECT

Detect attacks on your computer systems and networks and look for potential data breaches before the damage is done.

Even though you've taken steps to ***Protect*** *your data by beefing up your hardware and software defenses, you still need to monitor those defenses.*

Just as you need smoke detectors, fire alarms and fire extinguishers in your facility, it's imperative that you have the tools to quickly **Detect** a breach and quickly take action before a "fire" gets out of hand.

It's less costly to take steps now to monitor and detect attempts than to wait until the authorities or your credit card processor notify you there's a breach.

Consider first setting up a web-log analysis tool that allows you to set a baseline of what your systems look like when they're running securely.

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

Detection procedures and tools can shorten the time it takes to learn of an attack or breach. The longer an attack goes unnoticed, the longer criminals have access to your systems and operations.

The faster you respond to a breach, the more likely you are to contain most — if not all — of the damage.

CHECK YOUR SYSTEMS REGULARLY TO DETECT ABNORMAL ACTIVITY SUCH AS:

❑ **Large files being transferred out of your POS system**, e.g., customer credit card numbers you keep on file in case of a chargeback investigation.

❑ **Unexpected Internet site** and network traffic.

❑ **Unknown files, software and devices** installed on your systems.

❑ **Disabled antivirus programs.**

❑ **Increased after-hours activity** on your systems.

❑ **Unknown applications** that launch automatically when you reboot.

RESPOND

Plan how to respond to a data breach or cyberattack on your systems or networks.

Using the NIST Cybersecurity Framework, you've learned to **Identify** *digital risks to your business,* **Protect** *your computer systems, networks and data, and* **Detect** *intrusions. Now you need to plan how to* **Respond** *in a worst-case scenario.*

Preparing yourself to act will save you time, money, and stress, and mitigate further damage to your restaurant.

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

RESPONDING TO A DATA BREACH

- ❑ **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?
- ❑ **Are you required 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 should you call? Do you have their phone numbers?

Your answers will set the stage for your next steps. Most states have data breach notification laws you'll have to follow. 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 attack involves payment card data, your card brand will have specific guidelines for you to follow. You may be asked not to turn off, access or alter the compromised systems. You should preserve all logs, document all actions 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 in the event of a breach can save precious time.

Your first call after detecting an attack or breach should be to a lawyer who is well versed in cybercrime. After that, all activity should be run through the attorney. These experts will be able to work with you to mitigate the impact of potential lawsuits.

RECOVER

Putting a plan together in advance will help you recover faster after responding to a data security incident.

If your restaurant is taken down by a breach, how will you get back to normal?

The **Recover** function of the NIST Cybersecurity Framework not only helps you bounce back from potential disaster but also calls for learning. What lessons can you apply to your operations to avoid future breaches?

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

You need to consider, too, the financial resources it could 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 noted in prior sections of this series, returning to normal after a breach can be a lengthy process.

SOME QUESTIONS YOU SHOULD BE PREPARED TO ANSWER

- ❑ **Have you fulfilled all your legal obligations,** including notifying law enforcement and your customers?
- ❑ **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?

One key thing to remember about a data security plan built on the NIST framework is that it's never complete.

Like the HACCP plan that keeps your food safe, it requires constant tweaking as your operation changes and grows. Like adding a menu item to your HACCP plan, adding a new computer or software program, changing ISP vendors, or hiring a third-party customer loyalty program administer all require attention and changes to your data security plan.