

Cybersecurity 201

THE NEXT STEP



About This Guide

As a restaurant owner, you routinely safeguard things of value to your business. You put cash and receipts in a register or safe. You provide your employees with a safe place to work. You maintain the highest standards when selecting, storing and preparing food. You make sure your guests can securely navigate your restaurant and its parking area. You guard against any threats to your brand and reputation. Protection is just part of the job when you're a restaurant operator, and securing your data is no different.

Data security has become crucial to a restaurant operation's success. Although cybersecurity may seem like an overwhelming issue, there is a lot you can do to protect your restaurant against cyberattacks — and those security measures don't have to be complicated or expensive. Creating a cybersecurity plan starts with some basic, straightforward steps.

The National Restaurant Association's 2015 "[Cybersecurity 101: A Toolkit for Restaurant Operators](#)" guide highlighted five core "functions" (areas) of cybersecurity planning. "Cybersecurity 201: The Next Step" builds on our earlier guide to provide restaurant-specific guidance. A volunteer group of IT staff from some of the nation's top multi-unit restaurant companies collaborated to come up with action steps within each of the five areas of cybersecurity planning: **Identify, Protect, Detect, Respond** and **Recover**. The result — our Cybersecurity Framework for the Restaurant Industry — can help restaurant operators of all sizes and types protect themselves against cybercrime.

We hope you find the guide useful and we are grateful to the members of the National Restaurant Association's Information Technology Executive Study Group who generously devoted their time and expertise to create this guide.

Legal Disclaimer: The information provided here is a service to help guide your company's cybersecurity planning and assist you in managing risk. However, implementation of the information contained herein cannot guarantee that your business will not experience a data breach. We encourage you to consult with cybersecurity experts when developing your cybersecurity plans.

October 2017

TABLE OF CONTENTS

INTRODUCTION Cybercrime: A Growing Problem.....	1
CASE STUDIES Is This You? Meet the Restaurateurs.....	2
SECTION 1 Get Ready	7
SECTION 2 Cybersecurity Framework for the Restaurant Industry.....	11
APPENDICES:	
A) At a Glance: What's Urgent.....	43
B) Glossary	47
C) The NIST Framework versus the PCI Data Security Standard.....	48

SHARED VISION of the National Restaurant Association, National Restaurant Association Educational Foundation and State Restaurant Associations: We lead America's restaurant and foodservice industry by elevating its prosperity, prominence and participation, enhancing the quality of life for all we serve.

NRA MISSION: We serve our members by advancing and protecting America's restaurant and foodservice industry.

NRAEF MISSION: As the philanthropic foundation of the National Restaurant Association, we enhance the industry's service to the public through education, promotion of career opportunities, and community engagement.

INTRODUCTION

Cybercrime: A Growing Problem

These days, business planning for cybersecurity is just as important as planning for food safety or quality assurance. Whether you're a small restaurant operator or part of a large, well-known company, your systems can be compromised. No business is immune.

As we noted in 2015's "[Cybersecurity 101: A Toolkit for Restaurant Operators](#)," the digital age is transforming the way restaurants do business. Technology innovations have streamlined restaurant operations, reduced costs and attracted more guests. Many of those innovations are fueled by data. And whenever data is handled — via card payments, payroll and human resources records, inventory control, or loyalty programs — online criminals and hackers are lurking, waiting to attack where your operation is most vulnerable.

The good news is that you can do something about it. You can fight back. You can take steps to protect your operation and your

customers so you're less susceptible to data breaches and other criminal activity.

Preventive measures can make a big difference, and they don't necessarily require massive investments in new technology. It's often more a matter of thinking the right way about security than it is about purchasing expensive hardware or high-priced security services.

DOING SOMETHING IS BETTER THAN NOTHING

Cybersecurity can seem a bit overwhelming at first, but this guide will help you make sense of it. The worst thing you can do is nothing.

Reading the National Restaurant Association's "Cybersecurity 101" is a good first step to familiarize yourself with the basics of data security. In that guide, you'll learn about the Cybersecurity Framework that the [National Institute of Standards and Technology \(NIST\)](#)

developed in 2014. The NIST Framework is built around the five core functions of cybersecurity planning: **Identify, Protect, Detect, Respond** and **Recover**. It has become the go-to data-security resource for many companies. In fact, the technology research firm Gartner predicts that half of all U.S. businesses will use the Framework by 2020.

WHAT'S IN THIS GUIDE

Now that you've familiarized yourself with the NIST Cybersecurity Framework, "Cybersecurity 201" helps you move into action. We encourage you to read through each section:

- First, we'll introduce you to four hypothetical restaurant operators: Sam, Terri, William and Karen. Each has a lesson to share — and each ended up embracing the NIST Cybersecurity Framework for their planning.
- **Section 1: Get Ready.** It's important to adjust your thinking about cybersecurity. You need to look at cybersecurity as a continual process, not a checklist. You'll also need to evaluate the level of risk that's right for your operation; involve your team; and continually assess your progress.
- **Section 2: Cybersecurity Framework for the Restaurant Industry.** This is the real substance of our "Cybersecurity 201" guide. Our team of restaurant experts took the NIST Framework and customized it for the restaurant industry. We include our full Cybersecurity Framework for the Restaurant Industry in this section. It directly parallels the NIST Framework and explains how NIST's nearly 100 subcategories can apply in a restaurant setting.
- **Appendices.** Additional resources are included that may be helpful, starting with an at-a-glance listing of the actions our team has rated as most urgent. We've also included a glossary and brief overview of the Payment Card Industry Data Security Standard.

WHY ACT?

Data breaches carry huge costs

Restaurateurs can expect significant costs in the event of a data breach, including:

- **FEES AND PENALTIES.** If the breach involves payment card data, you'll likely face substantial fines from the card brands. That includes card-brand compromise fees, card-reissuing and monitoring fees, and fraud-reimbursement.
- **FORENSIC AUDITS.** You will likely need to hire an approved forensic investigator to find out what happened. Those costs can range from \$10,000 to more than \$100,000 per investigation, depending on the size, complexity and extent of the breach.
- **REMEDICATION.** Depending on what the forensic investigation finds, you may need to install expensive hardware and software and modify your network to remediate the vulnerabilities.
- **BREACH NOTIFICATION.** State laws set increasingly complex requirements about a business's responsibilities for informing customers in the event of a breach.
- **INEVITABLE LAWSUITS.** Once you inform guests or employees about a breach, that could trigger tort lawsuits for failure to protect, inadequate security and negligence.
- **INESCAPABLE BRAND DAMAGE.** For many businesses, holding onto customers after a breach can be among the biggest challenges.

Is This You?

Meet Sam, Terri, William and Karen, successful restaurateurs. You probably have a lot of things in common with them, but hopefully data-security problems aren't one of them.



Sam

The Payment Card Breach



Terri

The W-2 Theft



William

The Loyalty-Card Breach



Karen

The Ransomware Disaster



IS THIS YOU?

Sam

The Payment Card Breach

WHO

Sam is a successful, independent restaurateur. He has worked hard to create a fun, casual dining experience for his guests. He is proud of what he has accomplished. He taught himself to run the business, build a staff and put together a popular menu. His restaurant has been getting good reviews and is growing fast — maybe a little too fast.

Sam trusts his manager to make decisions about hiring and purchasing. He's noticed some slip-ups, but he chalks it up to growing pains. The place is packed every night, and the money has been good. So he doesn't worry.

THE PROBLEM

One day, Sam gets a call: his restaurant's data has been compromised. Someone has been stealing credit card numbers from his customers and fraudulently charged more than \$100,000 in the last three months. On top of that, his processor bank says he must submit to an expensive forensic audit. He faces thousands of dollars in fines from the card companies.

Sam has always prided himself on knowing everything about his restaurant — except he doesn't know who has access to the software that runs his office systems, which vendors service his POS machines, or the last time his hardware was upgraded.

Tomorrow, a forensics team will descend on his restaurant to ask a lot of questions. As he discusses what's happening with his manager, he realizes nothing much has been written down. He doesn't know which employees or former employees have passwords to his computers. Have the passwords ever been changed?

NEXT STEPS FOR SAM

Sam realized he'd been pretty careless. He was sure he completed his annual self-assessment questionnaire to meet the requirements of Payment Card Industry Data Security Standard (PCI DSS; see Appendix C for details), the security protocol for companies that accept credit and

debit cards from major card companies. But to be honest, he didn't pay much attention to it, either before or after he sent it to his card processor.

Unfortunately, he found that this incident was only the tip of the iceberg. If anyone on his team had been paying attention, they would have noticed months earlier a significant increase in unexplained activity in back-office systems — computers rebooting for no reason, strange software running in the background, unknown files that weren't there before, slowdowns in network data transfer. Too bad for Sam: his system was compromised long before today, and the cyber thieves had just been getting bolder ever since.

The problems could have started innocently enough. Perhaps his part-time bookkeeper opened a “phishing” email that contained a piece of malware (software aimed at damaging or disabling computers and computer systems). Phishing emails often look like legitimate vendor emails with “real” invoices attached. She may have clicked on the attachment, thinking it was a bill that needed to be paid, but instead it secretly downloaded software that gave hackers access to all of Sam's transactions. The problem was compounded by the lack of firewalls between trusted and untrusted systems, spam filters, and anti-virus and anti-spyware software on the bookkeeper's computer. The bookkeeper hadn't updated her accounting software in over a year, so she missed out on some important security patches.

THE REST OF THE STORY

Sam survived the forensics audit, but had to pay a substantial fine. He lost a fair amount of business because of the data breach. It has been a tough six months, but he is starting to bounce back.

He has hired a managed services provider to help him track his compliance with the PCI Data Security Standard. Sam and his team are now using the **National Institute of Standards and Technology's Cybersecurity Framework** to guide year-round cybersecurity planning. They meet regularly to evaluate their progress and make sure they are staying on top of the basic steps that will help them prevent and detect problems before they become a liability.



IS THIS YOU?

Terri

The W-2 Theft

WHO

Terri manages operations for a multi-store restaurant group in a growing metropolitan area. You might think she has the resources and staff to stay on top of cybersecurity, but Terri's day is filled with meetings and a million little details that go into operating across several locations.

She hired a security consultant two years ago to review her operations and make recommendations on data protection. The consultant created a plan and helped her hire outside firms to tighten security and establish controls on the use of the company's computer, inventory and HR systems. Terri put the plan in place and then turned her attention to other parts of the business.

THE PROBLEM

Terri wonders if her hands-off approach makes her company vulnerable. She recently heard about a company whose employees' W-2 forms had been hacked. "Why would anyone want those?" she thought. Easy: hackers can use the personal details to steal someone's identity.

After some reading, Terri discovered that W-2 attacks often focus on external systems, such as the vendors who handle employee onboarding. Terri always assumed her onboarding service providers had great security. In fact, they told her so when she signed the contract. But when she dug up the contract and waded through the legalese, Terri realized the contract was clear: if the vendor has a breach of the information involving Terri's employees, Terri is on the hook to inform the employees. Even worse, she's responsible for any legal claims that might result.

Terri's head spins. Her company is at a critical juncture. As they open more locations, the last thing they need is an expensive, embarrassing data breach that compromises her employees.

NEXT STEPS FOR TERRI

After talking to her consultant, Terri concludes she can't blindly rely on third-party vendors to handle security. She needs to exercise greater oversight to ensure her restaurant's systems truly are protected. She realizes her own staff is a critical defense against cybercrime. A third-party security program can't catch everything a well-trained and conscientious employee might see.

In reviewing her company's cybersecurity plan, she sees many of the risks can be managed in-house — by controlling Wi-Fi and internet connections, approving which suppliers and contractors have access to company systems, using firewalls to separate servers with sensitive data, and disabling inactive user accounts. She brings up cybersecurity at the next staff meeting and suggests taking a look at a framework to help organize all the different aspects of cybersecurity.

THE REST OF THE STORY

Terri initiated a thorough review of her company's cybersecurity procedures. It's a good thing she did. It turns out the company had been lax in enforcing password protections and safeguarding sensitive employee records and accounting systems. In fact, Terri asked an outside security firm to check her company's computers to ensure no malware had been installed.

After that scare, her management team decided to devote one meeting each quarter to cybersecurity. Her finance, HR and IT employees now meet monthly to go through the **National Institute of Standards and Technology's Cybersecurity Framework**, using its five core functions and dozens of subcategories to plot a course of action. They know they can't do it all at once — no one can — but the teams are charged with determining what's most important so they can tackle cybersecurity step by step.



IS THIS YOU?

William

The Loyalty-Card Breach

WHO

William, the CEO of a quickservice restaurant company, has his hands full. He runs popular and high-volume foodservice outlets at the airport, a sports stadium and the convention center. William's restaurants are well-known and well-loved for their generous loyalty programs that quickly reward his customers.

This week, William's company is handling three events at the stadium and one of the biggest trade shows of the year at the convention center. His business is bustling, and he's worried about logistics. Can his suppliers deliver? Does he have the staff to prepare and serve all those meals? Does he need additional cash registers?

THE PROBLEM

On the final day of the big trade show at the convention center, William's company is churning out the boxed lunches and tallying up new loyalty-card memberships and points. At the end of the day, he's high-fiving everyone on his team. It's been a great day for the business.

What William doesn't know is that cyber thieves had been exploiting a flaw in his loyalty-card vendor's platform. Instead of points being allocated to his best customers' accounts, hackers stole the information — and they've already sold it online. They've also grabbed his customers' loyalty program information, including their names, addresses, contact information, social media handles and buying history. William is mortified to know that information on his most valuable customers has been stolen. 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.

NEXT STEPS FOR WILLIAM

When William's partner, Sandy, heard what happened, she was livid. She said, "Come here; I want to show you something." She had been collecting information about cybersecurity and pushed a summary of the **National Institute of Standards and Technology's Cybersecurity Framework** in front of him. The Framework outlines the five core functions of cybersecurity. "This is where it starts," Sandy said. "You're not leaving this room until you commit to getting someone in here who can help us implement this."

REST OF THE STORY

William realizes he needs to pay close attention to the vendors he does business with, especially when they handle information about his customers. He, Sandy and their team now work with a consultant who is helping them through the **NIST Framework** — making sure they're aware of how to **Identify, Protect, Detect, Respond** and **Recover** from data-breach incidents.



IS THIS YOU?

Karen

The Ransomware Disaster

WHO

Karen is vice president of operations for a 20-unit casual-dining chain. She is responsible for overseeing day-to-day operations, including management of sales, human resources and purchasing.

Karen asked the marketing manager to find new ways for the chain to expand its profile and sales. The manager was tasked with handling the details, and Karen moved on to other responsibilities.

THE PROBLEM

The company's marketing manager thought she'd found the perfect way to promote the chain when she received an email asking her company to participate in "Restaurant Week." She clicked the email and unwittingly launched a cyberattack on the company. The downloaded malware began spreading through the network. An on-screen message said the system was hacked and that all proprietary information had been seized. It then made its way through the corporate network, freezing access to all inventory, management and production systems. The message said the hackers would release control of the information for thousands of dollars in bitcoin.

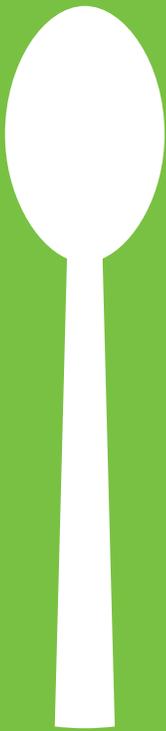
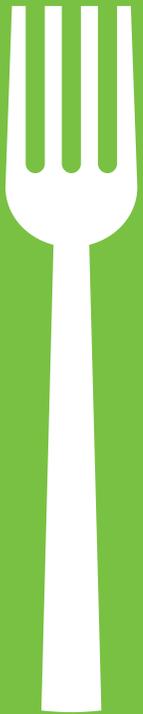
NEXT STEPS FOR KAREN

The company's IT team called in a consultant. The company had never had an incident of ransomware, and needed to know next steps. Could the consultant fix the problem? What would it cost? How would it affect sales? They had to know the best course of action: Should they pay the ransom and move on? What about contacting the police or FBI?

Getting the consultant to unfreeze the system cost thousands of dollars and several days of work. The company couldn't purchase supplies during the crisis because its automated system was disabled. Reservations couldn't be honored, and the loyalty program was inaccessible.

REST OF THE STORY

The consultant told Karen about the **National Institute of Standards and Technology's Cybersecurity Framework** and suggested she begin using it as a way to guide her planning. Karen now relies on the Framework to keep regular cybersecurity efforts top of mind for herself and her employees. Karen increased security measures, including changing passwords every 90 days and running weekly system scans. She made sure that all critical data is backed up and stored in a safe location, and that all systems have the latest security patches installed. She also implemented better security training for staff members. The company hasn't suffered another breach since.



SECTION 1
GET READY

SECTION 1: GET READY

Adjust Your Thinking

Get into the right mindset about cybersecurity

Creating a cybersecurity program for your restaurant involves taking some basic steps. You need to review the way you do business, assess where you're vulnerable, reduce risks, and conscientiously make improvements on an ongoing basis.

It's important to get into the right mindset as you start your planning. The **National Institute of Standards and Technology's Cybersecurity Framework** is a great approach to cybersecurity, but it's not a to-do list. It's a way of thinking about security that can be adapted and scaled to any operation. Before you begin your cybersecurity planning, make sure you're thinking about it the right way.

1

UNDERSTAND THE FIVE CORE "FUNCTIONS" OF CYBERSECURITY PLANNING

If you've read the National Restaurant Association's "[Cybersecurity 101](#)" guide, you're familiar with the five core functions (areas) of cybersecurity: **Identify, Protect, Detect, Respond** and **Recover**. Taken together, these functions provide a high-level, strategic view of the steps your restaurant needs to take to manage its cybersecurity risk. A good way to think of the core functions is to ask these five questions:



IDENTIFY

Which assets do I need to protect?



PROTECT

What safeguards are available? How can I implement and track them?



DETECT

How do I know if I'm experiencing a data breach?



RESPOND

How can I reduce the impact of an incident?



RECOVER

How do I quickly restore capabilities after a cyberattack?

2

LOOK AT THE FRAMEWORK IN ITS ENTIRETY

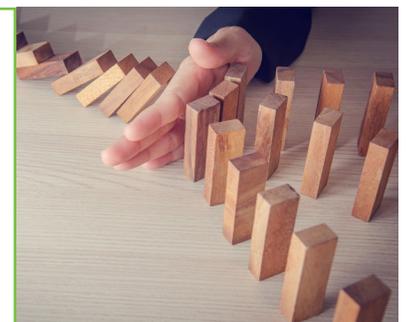
The NIST Framework — with its five functions and nearly 100 subcategories within those functions — has many parts and levels that all work together to help you reduce your risk of a cyberattack. Once you begin to see how the parts fit together, you'll understand the importance of developing a comprehensive plan.



3

UNDERSTAND YOU CAN'T ELIMINATE RISK COMPLETELY

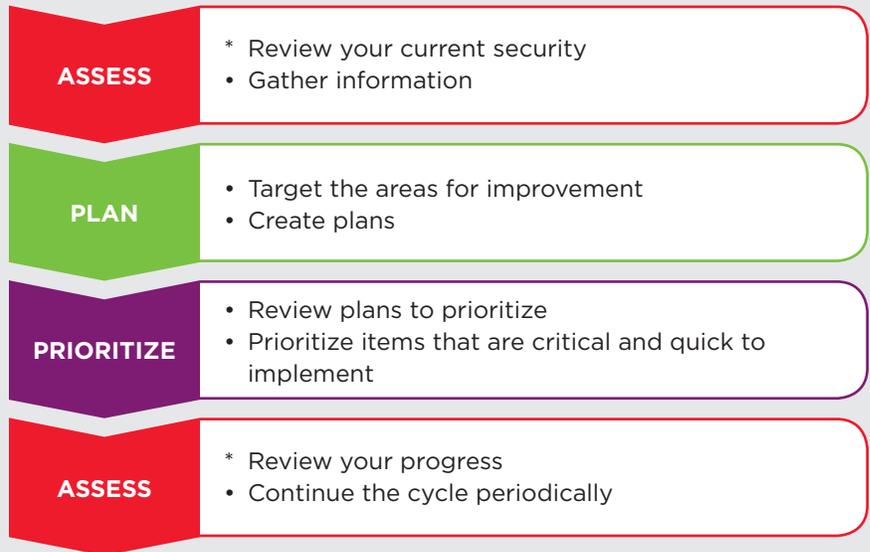
The NIST Framework is designed to reduce risk but can't totally eliminate it. The key to an effective cybersecurity program is to understand the costs and the benefits, and figure out what makes sense for your restaurant. Chances are you can live with some risk. So a good way to start is to eliminate risks that are easy to get rid of. The Framework shows you a way to do that. Your goal is to get to the optimum level of safety that makes sense for your restaurant.



4

PREPARE FOR CONTINUAL ASSESSMENT

One of the underlying concepts of the NIST Framework is that assessing your risk and working toward reducing it is a continual process.



5

REALIZE CYBERSECURITY PLANNING EVOLVES

You don't just check off boxes and put your plan on the shelf until next year. Cyber thieves have become increasingly sophisticated in attacking restaurants. You must become equally sophisticated and vigilant in taking security precautions.



6

AS CYBERSECURITY PLANNING EVOLVES, THE NIST FRAMEWORK WILL TOO

As the Department of Homeland Security has noted, "The Framework is a living document and will continue to be updated and improved as industry provides feedback on implementation. As the Framework is put into practice, lessons learned will be integrated into future versions. This will ensure it is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions." The National Restaurant Association is working with NIST and will continue to keep our members informed.



SECTION 1: GET STARTED

Action Steps

Now that you're familiar with the basics, take action

1

ASSESS YOUR SECURITY GOALS

Figure out where you are now in terms of cybersecurity, and where you want to be. The tactics and tools you employ must be tailored to your operation, taking into account your tolerance for risk and your available resources.



2

ENGAGE YOUR STAFF

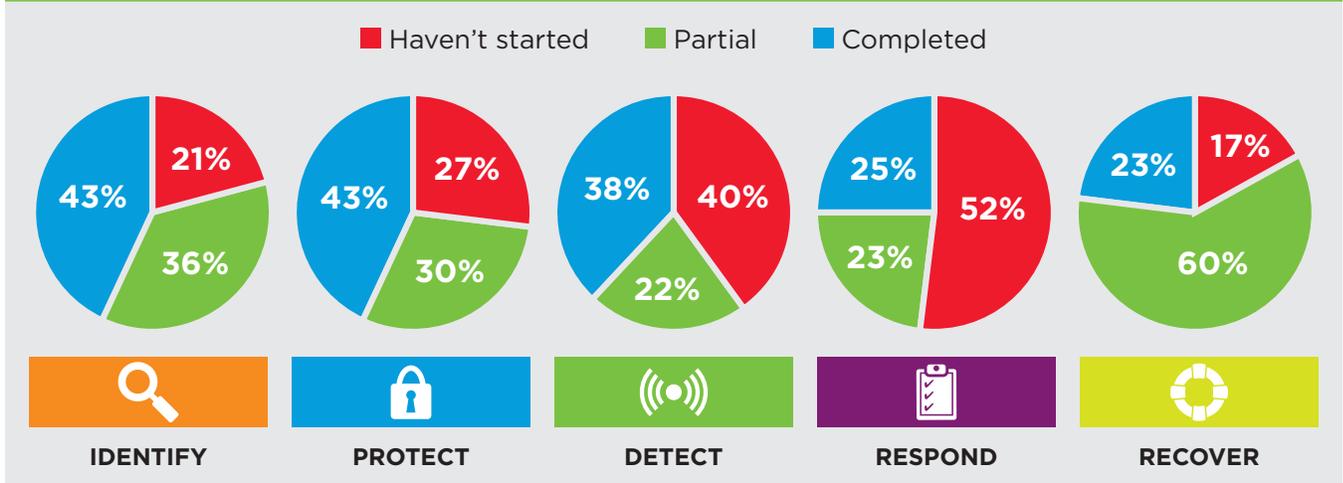
Review the entire Framework with your managers and teams. It may help to schedule regular meetings and tackle one section of the Framework at a time, going over the urgent items first. As you work your way through the Framework, keep employees informed about your progress and update them on the latest cybersecurity best practices.

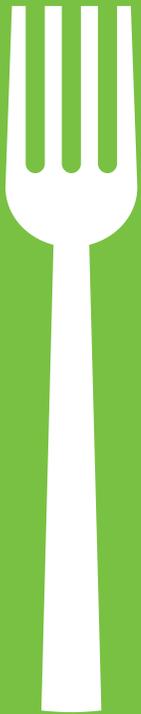


3

TRACK YOUR PROGRESS

With so many parts and pieces in the Cybersecurity Framework, you'll want to find an easy way to track your progress. You can create charts to track where you are (your current profile) compared to where you want to be (your target state). Use color-coding to highlight where you are across all five core functions. This simple chart illustrates a way you can track what you've started, what you've completed and what is yet to be done.





SECTION 2
**CYBERSECURITY
FRAMEWORK**
for the
**RESTAURANT
INDUSTRY**

SECTION 2

Cybersecurity Framework for the Restaurant Industry

Welcome to the nitty-gritty of our “Cybersecurity 201” guide. In this section, we provide a restaurant-specific version of the National Institute of Standards and Technology’s Cybersecurity Framework to help guide your restaurant’s cybersecurity planning.

We call it the **Cybersecurity Framework for the Restaurant Industry**. This tool helps restaurateurs work through NIST’s five core “functions” of cybersecurity — **Identify, Protect, Detect, Respond and Recover** — and incorporate this way of thinking into their cybersecurity plans. We developed this restaurant-specific version of the NIST Framework for smaller and mid-sized restaurant operators, but the information is equally helpful for larger operators.

HOW WE GOT HERE

The National Restaurant Association convened a team of cybersecurity experts from top restaurant companies in 2016. The team reviewed the NIST Cybersecurity Framework and customized it for the restaurant industry.

To come up with this restaurant-specific Cybersecurity Framework, our team:

- Reviewed the nearly 100 subcategories within the NIST Framework’s five core functions.
- Inserted restaurant-specific action steps and outcomes for each subcategory.
- Rated each subcategory for its level of importance and difficulty.



ABOUT THE CRITICALITY/DIFFICULTY RATINGS

Level of criticality/importance

Our team of restaurant security experts prioritized NIST’s subcategories to help you determine which actions will have the greatest impact on the security of your restaurant. Here’s how we have ranked the subcategories, with the highest priority first:

- **Urgent** – Actions required to maintain data security and prevent imminent breach
- **Critical** – Actions required to protect the integrity of the system and associated data
- **Important** – Actions required to meet compliance or regulatory requirements that impact the security of systems and associated data
- **Necessary** – Actions that enhance the security of systems and associated data
- **Complementary** – Actions that lead to a deeper level of security or maturity for systems and associated data

Level of difficulty

Our team also rated the difficulty of each action step:

- **Easy**
- **Moderate**
- **Difficult**

HOW TO USE THIS INFORMATION

You may want to set up a matrix to help you determine the relative level of difficulty and importance of the actions you take. For example, an action considered **Urgent** to your operation’s security could be rated **Easy** to achieve.

You may decide to focus on **Urgent** ●●●●● and **Critical** ●●●●● actions in the beginning. As you complete those, you could move on to **Important** ●●●●● and **Necessary** ●●●●● actions. Or, you may want to focus on the **Easy** actions first. The decision about how to proceed will be based on your operation’s risk assessment and target profile, and the security gaps you’ve identified that need to be filled.

We encourage you to share this Cybersecurity Framework with your team and cybersecurity consultants. As we noted in the previous section, it’s important to realize that your work is never done.

HOW TO APPLY THE FRAMEWORK IN YOUR RESTAURANT

The NIST Cybersecurity Framework is a way of thinking about cybersecurity. The **Cybersecurity Framework for the Restaurant Industry** is a framework for restaurateurs to think about cybersecurity.

Whether you're a small restaurant operator, mid-size operator, or large restaurant company, you can use our version of the Framework to help guide your planning. We recognize the process can feel daunting. With nearly 100 subcategories for companies to consider within the five core areas of **Identify, Protect, Detect, Respond** and **Recover**, it's a lot to absorb. A few reminders:

- Keep in mind that this is a process. You don't have to accomplish 100 percent of what's included here.
- Begin with a self-assessment. Look at the most critical items on our list and decide whether you're doing well on these or not. This will help you figure out where you need to start. Identify some critical items and start working through them.
- We've tried to show what these action steps would look like in a restaurant, and what level of effort it would take for an average restaurant operator to accomplish these. You can take many top-level actions on your own. As you dig deeper, you may need to ask for help. Whether you're doing this with your own resources, external resources, or a combination, we believe our framework will be useful in keeping you on the right path.

START WITH WHAT'S URGENT

Of the nearly 100 subcategories in the NIST Framework, our team of restaurant cybersecurity experts have rated 17 as **Urgent** ●●●●●.

In our team's opinion, these are the most important items to accomplish in your restaurant. You may want to start with these. (It's important to note that this is just a subset of a comprehensive set of security steps, and does not guarantee you won't experience a data breach.)

MAKING IT EASY:

- **Urgent subcategories at a glance:** Below is a list of the 17 items our team has rated **Urgent**. Appendix A on page 43 includes more details on these **Urgent** items, including some questions to ask in each area to help you get started.
- **Full list of all subcategories:** Our full Cybersecurity Framework for the Restaurant Industry follows in this section and includes each subcategory of the NIST Framework. We have added our team's assessment of the subcategory's importance/difficulty, how the actions might look in a restaurant setting and what outcomes you can expect if you accomplish these.

Identify

- Organizational communication and data flows are mapped.
- Dependencies and critical functions for delivery of critical services are established.
- Legal and regulatory requirements regarding cybersecurity, including privacy and civil-liberties obligations, are understood and managed.
- Threats, both internal and external, are identified and documented.

- Risk management processes are established, managed and agreed to by organizational stakeholders.

Protect

- Remote access is managed.
- Access permissions are managed, incorporating the principles of least privilege and separation of duties.
- Network integrity is protected, incorporating network segregation where appropriate.

- Physical and information security personnel understand roles and responsibilities.
- Communications and control networks are protected.

Detect

- The physical environment is monitored to detect potential cybersecurity events.
- Malicious code is detected.

Respond

- Response plan is executed during or after an event.
- Information is shared consistent with response plans.
- Coordination with stakeholders occurs consistent with response plan.
- The impact of the incident is understood.

Recover

- Public relations are managed.

CYBERSECURITY FRAMEWORK FOR THE RESTAURANT INDUSTRY

How we've organized our Cybersecurity Framework for the Restaurant Industry: Our Cybersecurity Framework for the Restaurant Industry parallels the National Institute of Standards and Technology's Cybersecurity Framework exactly. For each of the NIST Framework's five functions — **Identify, Protect, Detect, Respond** and **Recover** — we've included all NIST categories and subcategories. We identify each category and subcategory using NIST's official designations and descriptions.

What we've added to the NIST Framework: Our team of restaurant cybersecurity added the following information for each NIST subcategory, to help restaurants better understand how each might work in a restaurant setting:

- **How to apply this action in your restaurant**
- **Anticipated outcomes if action is completed**
- **Criticality / difficulty levels**

CONTENTS

NIST Function	NIST Category	Page
 Identify	Asset Management (ID.AM)	15
	Business Environment (ID.BE)	16
	Governance (ID.GV)	18
	Risk Assessment (ID.RA)	19
	Risk Management Strategies (ID.RM)	20
 Protect	Access Control (PR.AC)	21
	Awareness and Training (PR.AT)	23
	Data Security (PR.DS)	24
	Information Protection Processes and Procedures (PR.IP)	27
	Maintenance (PR.MA)	32
	Protective Technology (PR.PT)	32
 Detect	Anomalies and Events (DE.AE)	34
	Security Continuous Monitoring (DE.CM)	35
	Detection Processes (DE.DP)	37
 Respond	Response Planning (RS.RP)	38
	Communications (RS.CO)	38
	Analysis (RS.AN)	39
	Mitigation (RS.MI)	39
	Improvements (RS.IM)	40
 Recover	Recovery Planning (RC.RP)	40
	Communications (RC.CO)	41

NIST CATEGORY: Asset Management (ID.AM)

The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy.

ID.AM-1 Physical devices and systems within the organization are inventoried

How to apply in your restaurant:

- 1) Develop a tagging system for all physical IT devices, including a simple system for identifying type of physical asset, i.e., CPU or peripheral.
- 2) Develop or use a third-party secure database to track physical devices based on the asset tagging, including a serial number and model information.
- 3) Record each hardware device in the inventory database, including location and ownership.
- 4) Within inventory, document asset value, depreciation time and ownership. If known, end of life should be included.
- 5) Note whether the asset was purchased or leased.
- 6) The term of warranty and option for renewal should also be stated in the inventory record.

Anticipated outcomes if action completed:

You should maintain a complete list of hardware devices and a process to keep your inventory updated. Key information should include type, serial number, model, location, warranty and owner.

CRITICALITY



DIFFICULTY



ID.AM-2 Software platforms and applications within the organization are inventoried

How to apply in your restaurant:

- 1) Develop documentation or use third-party secure database software to inventory all software.
- 2) Include licensing and other key information in your inventory, along with purchase date, implementation date and expiration/renewal dates.
- 3) If the software is subscription-based, include the terms of the subscription.
- 4) Include any other required licenses such as client access licenses (CALs) or related system requirements for use.

Anticipated outcomes if action completed:

You should maintain a complete list of all software in use and a process to keep your inventory updated. Key information should include type, name, version, license number, business use, purchase date and business owner.

CRITICALITY



DIFFICULTY



ID.AM-3 Organizational communication and data flows are mapped

How to apply in your restaurant:

- 1) Map your restaurant’s communication and data flow requirements, and draft network diagrams.
- 2) Update and revise your documents as changes are made and/or on a periodic basis.
- 3) An appropriate level of leadership (i.e., CIO, GC, CEO, etc.) should review and approve the network diagrams and business communications.
- 4) Keep network diagrams in a repository accessible by employees with the correct level of access as determined by management.

Anticipated outcomes if action completed:

Your operation should prepare and periodically update a document describing the information flow within the business and how IT software, hardware and personnel support that information flow. The document should describe how this information supports your business objective and describe the relative risk to the business.

CRITICALITY



DIFFICULTY



ID.AM-4 External information systems are catalogued

How to apply in your restaurant:

- 1) Document all external systems, and code the systems for tracking, including type of system, data risk and locations.
- 2) Update documentation of all external systems whenever there are changes to those systems.
- 3) Annually review the documentation on external systems and include it in your audits.

Anticipated outcomes if action completed:

You should create and maintain a document that catalogs all external systems that contain sensitive and critical data and/or support critical business objectives.

CRITICALITY



DIFFICULTY



Asset Management (ID.AM) continued

ID.AM-5 Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value

How to apply in your restaurant:

- 1) Create a scoring system to identify the most critical to least critical technology systems.
- 2) List information systems from the most confidential and sensitive data to the least.
- 3) Determine the business value for each system.

Anticipated outcomes if action completed:

Prioritize your technology resources based on type of system, importance in achieving the business objective and value provided to the business. The priority can provide guidance to securing and upgrading your technology.

CRITICALITY



DIFFICULTY



ID.AM-6 Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

How to apply in your restaurant:

- 1) Develop roles and responsibilities for your employees and third parties regarding information systems and cybersecurity. All information systems and equipment should be included.
- 2) Your procedures may include a definition of information systems (i.e., networks, software and the data they produce) and equipment (cell phone, laptops, etc.), ownership (i.e., owned by the company), descriptions of overall expectations and proper use (business and/or limited personal use), inappropriate/misuse (violations of policies or laws) and disciplinary actions.
- 3) The procedures should be documented and retained in a location accessible to all employees or physically distributed (via intranet, break rooms, employee handbook, orientation packet, code of conduct, etc.). For third parties, the content should be included in appropriate supplier/vendor codes of conduct or in contractual agreements.

Anticipated outcomes if action completed:

Establish, document and communicate the cybersecurity roles and responsibilities of employees and third parties. These activities allow the organization to communicate expectations and proper use of information systems and assets.

CRITICALITY



DIFFICULTY



🔍 NIST CATEGORY: Business Environment (ID.BE)

The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

ID.BE-1 The organization’s role in the supply chain is identified and communicated

How to apply in your restaurant:

- 1) Identify and understand your restaurant’s and vendor partners’ role in each step of the supply chain.
- 2) Communicate the roles and responsibilities to all parties in the supply chain. In particular, those responsible for the vendor relationship should understand and know their role and the organization’s responsibility in managing security with that vendor.
- 3) ID.AM-6 (above) provides input to this item for identifying and communicating roles and responsibilities.

Anticipated outcomes if action completed:

Key business activities are identified, prioritized and communicated to help inform cybersecurity and risk-management decisions based on criticality to the business.

CRITICALITY



DIFFICULTY



Business Environment (ID.BE) continued

ID.BE-2 The organization’s place in critical infrastructure and its industry sector is identified and communicated

How to apply in your restaurant:

- 1) Document and communicate the infrastructure that supports the critical business activities identified in ID.BE-1 (above).
- 2) Clearly understand and communicate the responsibilities of your organization and its vendor partners for maintaining that infrastructure, and use that information in making cybersecurity and risk-management decisions. ID.AM-6 can provide input for identifying and communicating roles and responsibilities for critical infrastructure. (This item serves as input to ID.RM-3 below.)

Anticipated outcomes if action completed:

By understanding the infrastructure (technology in particular) critical to your business activities, you will be able to make informed cybersecurity risk-management decisions.

CRITICALITY



DIFFICULTY



ID.BE-3 Priorities for organizational mission, objectives, and activities are established and communicated

How to apply in your restaurant:

- 1) Document and prioritize your business activities to determine processes, technology and stakeholders that are key to achieving the organization’s objectives.
- 2) Communicate the priorities to align priorities and decision-making across the organization.

Anticipated outcomes if action completed:

Prioritizing your key business activities will help align cybersecurity, risk assessment and risk-management activities.

CRITICALITY



DIFFICULTY



ID.BE-4 Dependencies and critical functions for delivery of critical services are established

How to apply in your restaurant:

- 1) Create a list of services that are critical to running your business.
- 2) Document and communicate any technology, vendor relationships or service providers that are required to deliver those services.
- 3) Determine which services you are dependent on and your alternatives if those services are not available.

Anticipated outcomes if action completed:

You and your staff understand what critical services are needed to run your business and what key functions are needed to provide those services.

CRITICALITY



DIFFICULTY



ID.BE-5 Resilience requirements to support delivery of critical services are established

How to apply in your restaurant:

- 1) Document your requirements for delivery of critical services, including hours required to be available, maximum amount of time service cannot be available and how to deal with unavailability.
- 2) Include alternate ways of delivering services.
- 3) Include ways to deliver services temporarily and requirements for full delivery of services.

Anticipated outcomes if action completed:

By documenting the requirements for delivery of critical services, including how to handle and communicate their unavailability, you build resilience into your business processes.

CRITICALITY



DIFFICULTY



NIST CATEGORY: Governance (ID.GV)

The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

ID.GV-1 Organizational information security policy is established

How to apply in your restaurant:

- 1) Determine the regulatory and legal requirements for the restaurant’s security and include this information in your security policies.
- 2) Update your security policies on a periodic basis.
- 3) An appropriate level of leadership (i.e., CIO, GC, CEO, etc.) should review and approve all information security policies.
- 4) Communicate the policy to all appropriate company employees (annually is recommended).
- 5) Maintain information security policies in a repository accessible by employees.

Anticipated outcomes if action completed:

Establishing an information security policy will educate employees on regulatory requirements and the importance of security. Your policies should include employee roles and responsibilities and expectations of conduct. Information security policies should be communicated throughout the organization.

CRITICALITY



DIFFICULTY



ID.GV-2 Information security roles & responsibilities are coordinated and aligned with internal roles and external partners

How to apply in your restaurant:

- 1) The IT subject matter expert in partnership with HR and functional areas (i.e., finance, legal, supply chain, operations) should establish the roles and responsibilities of employees and external partners for the use and access of company information systems.
- 2) IT should map internal roles and external partners to information systems. Ensure that the appropriate roles are aligned with the required information systems and equipment.
- 3) Job descriptions should note the information system(s) required to complete job duties. External partner agreements, contracts, statements of work or other documents should include the information systems required to complete business activities.

Anticipated outcomes if action completed:

Clearly document, communicate and align security roles and responsibilities within the organization and between the organization and any third-party providers. Maintain appropriate levels of access to systems or databases based on roles.

CRITICALITY



DIFFICULTY



ID.GV-3 Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed

How to apply in your restaurant:

- 1) IT subject matter experts should be well informed of ever-changing industry standards and regulatory requirements, and provide ongoing updates to the organization.
- 2) IT subject matter experts should meet at least annually to discuss regulations and potential risks to the organization (see ID.RM-1).
- 3) Management should review requirements and risks to determine organizational risk tolerance and if additional controls are needed.

Anticipated outcomes if action completed:

The organization should be mindful of the constantly changing legal environment and industry standards related to cybersecurity. Subject matter experts must communicate and inform the organization of changes that impact the business and allow management to assess risk tolerance and determine if additional controls should be implemented.

CRITICALITY



DIFFICULTY



Governance (ID.GV) continued

ID.GV-4 Governance and risk management processes address cybersecurity risks

How to apply in your restaurant:

- 1) Meet with your board and/or management team at least annually to discuss risks to the company, including cybersecurity risks.
- 2) The discussion should include all potential cybersecurity risks, risk response plans and risk tolerance. Document the discussion and responses for review during the next meeting.
- 3) Ensure that your board and management are aligned on the risk level of cybersecurity in the organization, risk responses and risk tolerance.

Anticipated outcomes if action completed:

Cybersecurity risk management should be a part of the organization's regular risk-management processes and should include at least an annual executive level review of risk tolerance and risk response plans.

CRITICALITY



DIFFICULTY



NIST CATEGORY: Risk Assessment (ID.RA)

The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

ID.RA-1 Asset vulnerabilities are identified and documented

How to apply in your restaurant:

- 1) Review the network diagrams to assess and document vulnerabilities (see ID.AM-3).
- 2) Document the organization's controls for each risk/vulnerability compared to and in accordance with best practices and regulatory requirements.
- 3) Leadership (CIO, GC, CEO, etc.) should review the documentation and controls.
- 4) Review the network and asset vulnerabilities and reassess them whenever changes are made (at least quarterly).

Anticipated outcomes if action completed:

Establish a regular process to identify and review potential risks/vulnerabilities of key technologies, and discuss vulnerabilities and mitigation plans with the appropriate level of management.

CRITICALITY



DIFFICULTY



ID.RA-2 Threat and vulnerability information is received from information sharing forums and sources

How to apply in your restaurant:

- 1) Review ID.AM-1 and ID.AM-2 to identify threat-protection systems available to the organization.
- 2) Consult with the providers of threat-protection systems to determine whether automated vulnerability updates are available. Ask about data sources your staff can use to stay current on risks.
- 3) As part of your risk management strategy, evaluate options for automated updates and determine their suitability.
- 4) Assign responsibility to relevant team members for regularly reviewing external data sources appropriate to each individual's role.

Anticipated outcomes if action completed:

Identify external data sources to obtain a comprehensive and current view of technology-related risks. Consider sources available both in bulletin form for review by individuals and those that automatically update your threat-protection systems (anti-virus, security-incident event management, intrusion detection, etc.).

CRITICALITY



DIFFICULTY



Risk Assessment (ID.RA) continued

ID.RA-3	Threats, both internal and external, are identified and documented	<i>How to apply in your restaurant:</i>	<ol style="list-style-type: none"> 1) Determine sources of information about threats (industry resources like the National Restaurant Association, external sources identified in ID.RA-2, providers of threat-protection systems and internal subject matter experts). 2) Establish a structure for gathering and documenting threat information that complements the needs of all steps in the risk assessment process. 	<i>Anticipated outcomes if action completed:</i>	Develop a list of technology threats to your operation and update them on a regular basis. This covers all threats, both outside and within the organization, those of a technical nature and those of a human nature. You do not need to consider the actual risk or impact associated with these threats — that will be addressed by other elements of the overall risk assessment strategy.	CRITICALITY ●●●●●	DIFFICULTY ●●●
ID.RA-4	Potential business impacts and likelihoods are identified	<i>How to apply in your restaurant:</i>	<ol style="list-style-type: none"> 1) IT subject matter experts review the network diagrams to identify potential business impacts and likelihoods. 2) Management (CIO, GC, CEO, etc.) reviews the assessment. 	<i>Anticipated outcomes if action completed:</i>	Your organization reviews the impact and likelihood of a cybersecurity threat based on your unique business environment.	CRITICALITY ●●●●●	DIFFICULTY ●●●
ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	<i>How to apply in your restaurant:</i>	<ol style="list-style-type: none"> 1) IT subject matter experts rank the identified business impacts and likelihoods based on the risk. 2) Management (CIO, GC, CEO, etc.) reviews the assessment. 	<i>Anticipated outcomes if action completed:</i>	Your organization ranks the business risk from low to high based on known cybersecurity information.	CRITICALITY ●●●●●	DIFFICULTY ●●●
ID.RA-6	Risk responses are identified and prioritized	<i>How to apply in your restaurant:</i>	<ol style="list-style-type: none"> 1) IT subject matter experts identify the risk responses and prioritize them based on their impact on the business. 2) Management (CIO, GC, CEO, etc.) reviews the assessment. 	<i>Anticipated outcomes if action completed:</i>	Based on the risk ranking, your organization identifies and prioritizes the responses.	CRITICALITY ●●●●●	DIFFICULTY ●●●

🔍 NIST CATEGORY: Risk Management Strategy (ID.RM)

The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

ID.RM-1	Risk management processes are established, managed, and agreed to by organizational stakeholders	<i>How to apply in your restaurant:</i>	<ol style="list-style-type: none"> 1) Establish a schedule for leadership to review risk assessment details whenever they are updated. 2) Decide which risks will be reviewed by the leadership team (all risks? certain priorities?). 3) For those risks that are reviewed, document the response and rationale and then share with all relevant parts of the organization. 	<i>Anticipated outcomes if action completed:</i>	Establish a risk-assessment process with regular reviews by key members of your organization.	CRITICALITY ●●●●●	DIFFICULTY ●●●
----------------	---	---	---	--	---	-----------------------------	--------------------------

Risk Management Strategy (ID.RM) continued

ID.RM-2 Organizational risk tolerance is determined and clearly expressed

How to apply in your restaurant:

- 1) Review the risk responses (ID.RA-6) according to the schedule and process outlined by ID.RM-1.
- 2) Document planned actions (or inaction) for each risk response.
- 3) Review the risk tolerance represented by the approved mitigation activities to ensure consistency and appropriateness.
- 4) Communicate the overall plan and supporting tolerance posture to those responsible for execution.

Anticipated outcomes if action completed:

You will gain a clear understanding of which risks will be mitigated, which will be accepted and those in-between. You will also have these risks documented for use during the risk-management process.

CRITICALITY



DIFFICULTY



ID.RM-3 The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis

How to apply in your restaurant:

- 1) As part of your overall risk-management strategy, regularly consult with peers in other organizations (if possible) and industry resources (e.g., the National Restaurant Association) to stay abreast of evolving industry-specific risks.

Anticipated outcomes if action completed:

Consider those risks specific or unique to the restaurant industry and those that are based on the criticality of the technology's role in your business.

CRITICALITY



DIFFICULTY



NIST CATEGORY: Access Control (PR.AC)

Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

PR.AC-1 Identities and credentials are managed for authorized devices and users

How to apply in your restaurant:

- 1) Require unique accounts for each individual who accesses a POS terminal.
- 2) Require unique credentials for each user who logs on to network devices.
- 3) Regularly review users for completeness and appropriateness of access (quarterly is recommended).

Anticipated outcomes if action completed:

Require unique individual credentials for each user who accesses your POS, network or computer devices. This includes both internal access and third-party service providers. Regularly review accounts to validate that the user listing is accurate and timely. Remove access immediately upon separation. Do not authorize shared accounts to log on to applications, servers or network devices.

CRITICALITY



DIFFICULTY



PR.AC-2 Physical access to assets is managed and protected

How to apply in your restaurant:

- 1) Keep an inventory of unused devices in a secure area.
- 2) Conduct an ongoing inventory of IT assets to ensure that all assets are tracked and accounted for.

Anticipated outcomes if action completed:

All POS devices, network devices and computer devices are either stored in a secure location such as a secured office or data center or are regularly inventoried to monitor access. Your IT person should check devices that are unaccounted for before returning them to inventory or production usage. This includes inventory stored by external service providers.

CRITICALITY



DIFFICULTY



Access Control (PR.AC) continued

PR.AC-3 Remote access is managed

How to apply in your restaurant:

- 1) Manage and log all remote access of your systems by internal management or support teams.
- 2) Require and log unique individual logins for remote access by third-party providers.
- 3) Manage and log third parties that have data connectivity for remote data collection. Limit access to only the specific application/hardware required.

Anticipated outcomes if action completed:

Remote access includes internal business connections, service providers and third-party data connections. All of these connections are required to have unique credentials for each user with access. All access should be limited to only the hardware, applications or data required. All activities performed remotely should be logged. All access to the Payment Card Industry (PCI) cardholder data network should require two-factor authentication.

CRITICALITY



DIFFICULTY



PR.AC-4 Access permissions are managed, incorporating the principles of least privilege and separation of duties

How to apply in your restaurant:

- 1) Limit access privileges to the least necessary to perform a job.
- 2) Limit administrative or super user access to the fewest users possible.
- 3) Do not give users the ability to make changes to both development and production environments.

Anticipated outcomes if action completed:

Manage and document the roles and level of access for each individual user with access to your systems. Closely guard administrative and super-user accounts and only share them with trusted employees. Provide the least amount of access required to perform a job. Segregate duties to separate development and testing from production. For smaller operations that do not have dedicated testing environments, use a documented approval process for the time period when changes are pushed into production environments. Privileged accounts may be set with access only for the amount of time required to complete tasks. A valid approach is to permit access for 24 hours with approval for a specific activity.

CRITICALITY



DIFFICULTY



PR.AC-5 Network integrity is protected, incorporating network segregation where appropriate

How to apply in your restaurant:

- 1) Use physical or virtual firewalls to separate critical systems from network applications.
- 2) Run wireless networks on separate physical or virtual networks to enhance security.
- 3) Use technologies such as virtual local area networks (VLANs) or virtual routing and forwarding (VRF) to separate applications at the network layer.

Anticipated outcomes if action completed:

Access to all networks, both wired and wireless, should be secured through the implementation of physical firewalls. Technologies such as a stateful firewall (a network firewall that tracks the operating state and characteristics of network connections conversing it) can also be used to segregate network traffic for critical applications. Firewalls make it more difficult for breaches to spread across network

CRITICALITY



DIFFICULTY



NIST CATEGORY: Awareness and Training (PR.AT)

The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

PR.AT-1 All users are informed and trained

How to apply in your restaurant:

- 1) Disseminate security policies to all applicable users.
- 2) Perform annual reviews of all policies, and provide approved versions to all applicable users.
- 3) Provide security-related training to all applicable users (based on position) on a regular basis.
- 4) Train new users (based on position) on security-related policies upon hire.
- 5) Acquire sign-off from all users at least annually.

Anticipated outcomes if action completed:

All users play a critical role in information security. But they cannot assist with security if they do not know anything about security. Knowledge is the key.

CRITICALITY



DIFFICULTY



PR.AT-2 Privileged users understand roles & responsibilities

How to apply in your restaurant:

- 1) Perform a risk analysis to determine the scope of training required for privileged users.
- 2) Create role-based training on privileged use requirements.
- 3) Prepare a training plan for all privileged users.
- 4) Acquire sign-off from all users at least annually.

Anticipated outcomes if action completed:

Privileged users present a unique challenge for IT security. Users need to be made aware of the responsibilities and accountability related to elevated rights. Examine security risks on a case-by-case basis and provide appropriate training based on your analysis. User involvement and knowledge is critical to a successful cybersecurity program.

CRITICALITY



DIFFICULTY



PR.AT-3 Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities

How to apply in your restaurant:

- 1) Create and approve a third-party security policy. Include a risk analysis specific to the typical third-party users for the business.
- 2) Review and approve the policy at least annually.
- 3) Acquire sign-off from all third-party users at least annually.
- 4) Contracts with third parties should clearly define roles and responsibilities for the third party and your company's security controls.

Anticipated outcomes if action completed:

Third-party users require additional security considerations due to the variety of potential configuration settings, hardware specifics and third-party policies. This adds additional levels of risk, and with that comes unique security considerations. Third-party users need to know what their roles and responsibilities are and how this influences your security program. This information is critical to ensure that they are assisting you with your security as well as their own.

CRITICALITY



DIFFICULTY



PR.AT-4 Senior executives understand roles & responsibilities

How to apply in your restaurant:

- 1) Prepare an executive overview of all polices in sections PR.AT-1, PR.AT-2 and PR.AT-3.
- 2) Provide an annual overview of the items in Step 1 to your senior staff.
- 3) Receive sign-off from all executive users at least annually.

Anticipated outcomes if action completed:

Your top people should receive a higher-level overview of the security policies and programs involved with training all end users in the organization. Senior buy-in for these programs can be critical to the success of your restaurant's security initiatives.

CRITICALITY



DIFFICULTY



Awareness and Training (PR.AT) continued

PR.AT-5 Physical and information security personnel understand roles & responsibilities

How to apply in your restaurant:

- 1) Include physical and information security personnel in all levels of information security. Provide them with documented procedures that include security practices and daily operational processes.
- 2) Include specific line responsibilities for security personnel to ensure guidelines are set for granting permissions to other users.
- 3) Review and require sign-off of all policies on a regular basis for security personnel.
- 4) Provide appropriate security training to all security personnel.
- 5) Determine levels of experience, expertise and certifications for selection and hiring of security personnel.

Anticipated outcomes if action completed:

Security personnel have the right to change both user permissions and security settings/configurations. Due to this advanced level of access, it is imperative that these personnel are selected carefully and provided an appropriate level of training and review. Any mistake at this level can be critical.

CRITICALITY



DIFFICULTY



🔒 NIST CATEGORY: Data Security (PR.DS)

Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.

PR.DS-1 Data-at-rest is protected

How to apply in your restaurant:

- 1) Limit data storage amounts and retention times to what is required for legal, regulatory and/or business requirements.
- 2) Maintain an inventory of where your critical data is stored (credit card, customer and employee personally identifiable information (PII), financial and intellectual property, etc.).
- 3) Protect data at rest as prescribed by compliance requirements (i.e., PCI, HIPAA), legal requirements (federal, state and local) and organizational standards. Protection methods may include encryption, access control, data masking/truncation and intrusion detection.
- 4) Delete data that is no longer required using a secure method, ensuring that it cannot be recovered by a forensic process or method.
- 5) Ensure that your data retention and disposal policies meet legal and compliance requirements.

Anticipated outcomes if action completed:

Data at rest is a significant exposure for companies if it is not properly protected. Minimize data storage to reduce risk. Provide access rights only when it supports business demands, legal requirements and compliance mandates. Restaurants must comply with data-at-rest protection requirements as determined by compliance mandates (i.e., PCI, HIPAA) and federal, state and local legislation.

CRITICALITY



DIFFICULTY



Data Security (PR.DS) continued

PR.DS-2 Data-in-transit is protected

How to apply in your restaurant:

- 1) Identify all locations where critical data (credit card, logon credentials, customer/employee personally identifiable information, etc.) is transmitted or received over a network.
- 2) Use strong cryptography and security protocols to safeguard critical data, based on an analysis,

Anticipated outcomes if action completed:

Critical data should be encrypted when it is transmitted over networks that could easily be accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of criminals who exploit these vulnerabilities to gain privileged access to critical data environments. To provide the most secure environment, both the data payload and transmission means should be encrypted. Encryption of just the transmission using transport layer security (TLS) or a secure sockets layer (SSL) does not provide optimal security. Established and reputable providers should manage your encryption and keys. The integrity of the encryption keys is critical to the security of the data.

CRITICALITY



DIFFICULTY



PR.DS-3 Assets are formally managed throughout removal, transfers, and disposition

How to apply in your restaurant:

- 1) Identify, inventory and label all critical assets, including servers, workstations, payment systems, network equipment, etc. Labels should include a unique identifier (such as a serial number), manufacturer, model and date put into service.
- 2) Establish a formal disposal/transfer policy supporting the secure destruction or sanitation of assets that may contain critical data.
- 3) Routinely inventory critical devices and perform inspections to assure assets are maintained in a secure manner and have not been tampered with. At a minimum, inventory your assets once a year.

Anticipated outcomes if action completed:

Identify and manage your assets consistent with their relative importance to your business objectives and risk strategy. Track assets from procurement, production and end of life to end of support and secure disposal.

CRITICALITY



DIFFICULTY



PR.DS-4 Adequate capacity to ensure availability is maintained

How to apply in your restaurant:

- 1) Determine capacity requirements (storage, bandwidth, CPU, power consumption, etc.).
 - Define required system performance to support your restaurant’s workloads.
 - Agree upon minimum levels of support, and test the system against defined business requirements.
- 2) Analyze your current capacity.
 - Monitor existing usage of system resources.
 - Record and track utilization of existing systems.
 - Understand historical capacity utilization and any available industry standard usage data (i.e., peak holidays for restaurants).
- 3) Plan for future capacity.

Anticipated outcomes if action completed:

Capacity is defined as the maximum amount or number that can be received or contained. For example, the amount of data that a computer hard disk can store is the disk’s capacity. Capacity management is supporting the optimum, cost-effective provisioning of services to match resources with business needs. Measurements should include all critical infrastructure components such as disk space, memory utilization, bandwidth consumption, processing threads, log sizes and more. A mature capacity management program will reduce downtime of systems and increase availability of systems through-out an organization.

CRITICALITY



DIFFICULTY



Data Security (PR.DS) continued

PR.DS-5 Protection against data leaks are implemented

How to apply in your restaurant:

- 1) Create a data classification policy that defines appropriate levels of protection for data. At a minimum, your policy should support required levels of protection as defined by legal and regulatory requirements, but also consider appropriate protections for all sensitive financial, personally identifiable information and intellectual property to ensure appropriate duty of care.
- 2) Institute data protection standards to safeguard data (allowable credit card data is encrypted per the current PCI standard, etc.).
- 3) Consider implementing technologies to prevent the inappropriate exfiltration (unauthorized transfer) of data, including data loss prevention, Internet content filtering and digital rights management.
- 4) Log and monitor the key systems and personnel that store, process and transmit sensitive data as defined by your company's data classification policy.
- 5) Consider background checks and drug screens for key personnel with access to sensitive information based upon the company's culture and legal tolerance.
- 6) Establish a hotline for employees and individuals outside the company to enable red-flag notification.

Anticipated outcomes if action completed:

A data classification framework will ensure that you are providing the appropriate level of protection for your company and appropriate legal and compliance standards. Training and awareness, background checks and company hotlines can also mitigate the risk of data leaks.

CRITICALITY



DIFFICULTY



PR.DS-6 Integrity checking mechanisms are used to verify software, firmware, and information integrity

How to apply in your restaurant:

- 1) Deploy technologies to assure the integrity of critical and sensitive information, including application and system resources such as file-integrity monitoring, application whitelisting, intrusion detection/prevention and firewalls.
- 2) Develop a policy for cryptographic key and certificate management, key retirement and rotation to ensure the integrity of keys that protect vital systems and information.
- 3) Secure audit trails so they cannot be altered and retain them based on compliance requirements (PCI DSS, SOX, etc.).
- 4) Institute change-detection procedures to alert personnel of unauthorized changes and provide guidance concerning changes that might impact the integrity of data and systems.

Anticipated outcomes if action completed:

Maintaining data integrity ensures that data can be recovered, searched and traced, and it improves connectivity, stability and performance. Data increasingly drives enterprise decision-making. Therefore, data integrity is a top priority for the restaurant industry. Data integrity can be compromised in a variety of ways, making data integrity practices an essential component of effective enterprise security protocols. Data integrity may be compromised through:

- Human error, whether malicious or unintentional
- Transfer errors, including unintended alterations or data compromise during transfer from one device to another
- Bugs, viruses/malware, hacking and other cyber threats
- Compromised hardware such as a device or disk crash
- Physical compromise to devices
- Theft

CRITICALITY



DIFFICULTY



Data Security (PR.DS) continued

PR.DS-7 The development and testing environment(s) are separate from the production environment

How to apply in your restaurant:

- 1) Separate development/test environments from production environments and put access controls in place to enforce separation.
- 2) Segregate duties between personnel assigned to the development/test environments and those assigned to the production environments.
- 3) Do not use production data (credit card, customer/employee personally identifiable information) for testing or development.
- 4) Remove test data accounts from production before going live.
- 5) Change control procedures related to security

Anticipated outcomes if action completed:

Development environments typically do not maintain the same level of security as production environments, so it is critical that you segregate the duties of these two environments. Prevent inappropriate access to ensure security features are not inadvertently or deliberately omitted or rendered inoperable, causing processing irregularities or malicious code to be introduced.

CRITICALITY



DIFFICULTY



NIST CATEGORY: Information Protection Processes and Procedures (PR.IP)

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

PR.IP-1 A baseline configuration of information technology/industrial control systems is created and maintained

How to apply in your restaurant:

- 1) Establish and adhere to configuration baselines for information systems and components, including:
 - Point-of-sale operating systems
 - Back-office server and workstation operating systems
 - Above restaurant servers, workstations, laptops and mobile devices
 - Network devices, e.g. firewalls, routers, switches
- 2) Leverage available automated mechanisms such as hardware and software inventory tools, configuration tools and network management tools to help maintain an up-to-date, complete, accurate and readily available baseline configuration of your information systems. For example, you can track version numbers on operating system applications, types of software installed and current patch levels.
- 3) Retain previous versions of baseline configurations to support rollback. Rollback baselines may include point-of-sale hardware, software, firmware, configuration files and configuration records.
- 4) Implement additional security controls for systems located in high-risk areas (such as publicly accessible point-of-sale systems in a casual dining environment) to counter the greater threat in such areas and the lack of physical security controls.
- 5) Ensure that point-of-sale systems conform to a baseline configuration that sufficiently protects systems in high-risk areas, i.e., one that has limited applications and additional hardening such as disabling exposed USB ports.

Anticipated outcomes if action completed:

Document and maintain a formally reviewed and agreed-upon set of baseline configurations for systems and system components, including communications and connectivity-related systems. Baseline configurations serve as a basis for future builds, releases and/or changes to information systems such as point of sale, restaurant servers and workstations, as well as laptops, desktops and mobile devices. Baseline configurations include information about systems such as standard software packages, current version numbers, patch information, configuration settings, parameters for operating systems and applications, network topology and the logical placement of these components within the overall system architecture. Maintaining baseline configurations requires creating new baselines as systems are upgraded and changed over time. NIST Special Publication 800-53 and the Center for Internet Security (CIS) secure configuration benchmarks are resources that can help you establish a comprehensive configuration baseline standard.

CRITICALITY



DIFFICULTY



Information Protection Processes and Procedures (PR.IP) continued

PR.IP-2 A System Development Life Cycle to manage systems is implemented

How to apply in your restaurant:

- 1) Establish a system development life cycle for the implementation or upgrade of software such as credit card processing, POS software, back-office software or network device software.
- 2) Establish a system development life cycle for the implementation or upgrade of hardware such as credit card processing terminals, POS hardware, back-office hardware and network devices.
- 3) Establish a system development life cycle for custom development of software such as point-of-sale software.
- 4) Ensure that your system development life cycle includes the entire life of your systems, from initiation, development, testing, QA and production to disposal.

Anticipated outcomes if action completed:

The system development life cycle is comprised of a number of clearly defined and distinct work phases that are leveraged to provide the foundation for the successful development, implementation, testing and operation of information systems. Ensure that security requirements such as information security, threats, vulnerabilities, adverse impacts and risk to critical missions/business functions are incorporated into your information systems. Your development team should possess the necessary security expertise and skills to ensure that needed security capabilities are effectively integrated into the information system.

CRITICALITY

DIFFICULTY

PR.IP-3 Configuration change control processes are in place

How to apply in your restaurant:

- 1) Ensure that configuration change control processes are in place for all hardware changes (including new and replacements) to credit card processing terminals, POS hardware, back-office hardware and network devices.
- 2) Ensure that configuration change control processes are in place for all software changes (including new and replacements) to credit card processing software, POS software, back-office software and network device software.
- 3) Ensure that configuration change control processes are in place (including new and replacements) for third parties such as external service providers to hardware and software.

Anticipated outcomes if action completed:

Configuration change control processes should include testing, documentation, review, evaluation of security impact and approval prior to making any modifications to information systems. Qualified personnel should analyze all changes to verify that modifications do not adversely impact your restaurant's information security. The IT Infrastructure Library (ITIL) is a resource that can help you establish a comprehensive change management program.

CRITICALITY

DIFFICULTY

PR.IP-4 Backups for information are conducted, maintained, and tested periodically

How to apply in your restaurant:

- 1) Develop a comprehensive backup strategy as part of your contingency planning.
- 2) Periodically test (at least annually) your backups to ensure their integrity.
- 3) Store backups at an alternate storage site so that backups of critical infrastructure may be obtained in the event the primary storage facility is unavailable.
- 4) Encrypt backups of sensitive data such as credit card and personally identifiable information.

Anticipated outcomes if action completed:

Maintaining and testing user and system-level information backups is an important component of a robust business continuity and contingency plan. Data on systems could be lost due to a variety of reasons such as hardware failure, software or system corruption, malware and virus infections or natural disasters. For these reasons, systems should be backed up on a daily basis using available backup software and automated capabilities. Once backed up, the data should be stored at an alternate storage site. The alternate site should have information security safeguards equivalent to that of the primary site and the ability to retrieve the data. The backup information should be tested, at a minimum, annually in order to verify the reliability and integrity of the backup. Sensitive information such as personally identifiable information and credit card data should be encrypted at rest regardless of the backup medium type.

CRITICALITY

DIFFICULTY

Information Protection Processes and Procedures (PR.IP) continued

PR.IP-5 Policy and regulations regarding the physical operating environment for organizational assets are met

How to apply in your restaurant:

- 1) Keep your back-of-house file server in a place that minimizes damage from physical and environmental hazards.
- 2) Minimize the opportunity for unauthorized access to the file server by keeping the system behind a locked door.
- 3) If information systems are concentrated in a data center or server room, the data center or room should be equipped with the following: (a) emergency power shutoff capabilities, (b) emergency lighting, (c) water damage protection, (d) fire suppression and detection devices, and (e) temperature and humidity controls. The room should be in a location that minimizes potential damage from physical and environmental hazards.
- 4) Include a review of the physical data center environment in your contracts and relationships with third-party service providers.

Anticipated outcomes if action completed:

This control applies primarily to facilities containing concentrations of information system resources, including data centers and server rooms, but it may also apply to restaurant installations. Your policies should include measures for protection against environmental factors and installing specialized equipment and devices to monitor and control the facilities environment. Manage your facilities in line with appropriate laws and regulations, technical and business requirements, vendor specifications, and health and safety guidelines.

CRITICALITY



DIFFICULTY



PR.IP-6 Data is destroyed according to policy

How to apply in your restaurant:

- 1) During a POS or back-office-system refresh, sanitize (destroy) end-of-life hard drives prior to the equipment leaving your restaurant's possession.
- 2) Sanitize above restaurant system storage and backup media to remove sensitive team member, guest and payment data prior to reusing or releasing it.
- 3) If a restaurant system service call requires a hard drive replacement, remove sensitive data if the drive is still functional. If the hard drive is not operating at a capacity that allows for sanitization, destroy the drive and render sensitive data unreadable.
- 4) Archive or destroy documents such as employee records containing personally identifiable information that are no longer required after a team member has been terminated.

Anticipated outcomes if action completed:

Digital and non-digital media containing sensitive information should be sufficiently sanitized or destroyed, according to policy prior to disposal, reuse or release out of organizational control. Department of Defense 5220.22-M Clearing and Sanitization Guidelines and NIST Special Publication 800-88 are good references for recommended approaches and methods.

CRITICALITY



DIFFICULTY



Information Protection Processes and Procedures (PR.IP) continued

PR.IP-7 Protection processes are continuously improved

How to apply in your restaurant:

- 1) Review and improve your protection processes based on your experience with the processes.
- 2) Review and revise protection processes periodically to address federal legislation, executive orders, directives, regulations, policies, emerging threats, vulnerabilities, attack methods or updates to frameworks, including NIST, PCI, ITIL, etc.
- 3) Review and revise protection processes to address changing security requirements or changes to the environment such as new applications, systems or processes.
- 4) Review and improve protection processes periodically to take advantage of new technologies.

Anticipated outcomes if action completed:

Protection processes change over time. Carefully review and revise them periodically to reflect experience gained from using the processes and address any changes that may affect the security of protected data. The review process should take into account:

- New federal legislation, executive orders, directives, regulations or policies
- Changing security requirements or changes to the environment such as new applications, systems or processes
- Emerging threats, vulnerabilities and attack methods
- Availability of new technologies
- Changes or updates to frameworks, including NIST, PCI, ITIL, etc.

CRITICALITY
● ● ● ● ●

DIFFICULTY
● ● ●

PR.IP-8 Effectiveness of protection technologies is shared with appropriate parties

How to apply in your restaurant:

- 1) Share with appropriate parties the extent to which the security framework has been implemented.
- 2) Share with appropriate parties the results of all tests performed on security systems and procedures.
- 3) Share with appropriate parties the results of regular internal and external vulnerability scans and penetration testing.

Anticipated outcomes if action completed:

Share the effectiveness of protection technologies and procedures with appropriate parties, including:

- Company executives
- All individuals responsible for managing protection technologies
- Auditors (internal and external)
- Card processors/service providers

CRITICALITY
● ● ● ● ●

DIFFICULTY
● ● ●

PR.IP-9 Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed

How to apply in your restaurant:

- 1) Create a response and recovery plan with procedures and points of contact for responding to a security event such as unauthorized physical or virtual access to protected systems, malware, data exfiltration, etc.
- 2) Create a recovery plan that contains procedures and points of contact for responding to a system outage. This may include outages related to an individual system or location, or enterprise-wide shared systems.

Anticipated outcomes if action completed:

A detailed plan provides the process for recovery in the event of a system failure, security breach or other types of disaster, such as natural disasters, terrorism, etc. Your plan should include how to respond to a failure/breach of both restaurant-level systems (such as the POS or payment networks) and any enterprise systems (such as payroll or email systems). Include points of contact for support and procedures to follow to prevent the failure/breach from affecting other systems and to ensure continuity of service. Points of contact will vary based on regulatory requirements for individual jurisdictions such as state, county, etc.

CRITICALITY
● ● ● ● ●

DIFFICULTY
● ● ●

Information Protection Processes and Procedures (PR.IP) continued

PR.IP-10 Response and recovery plans are tested

How to apply in your restaurant:

- 1) Create a recovery plan with procedures and points of contact for responding to a system outage. Include outages related to an individual system or location and enterprise-wide shared systems.
- 2) Perform and document annual tests of your recovery plan. Capture lessons learned and remediate key findings from the testing.

Anticipated outcomes if action completed:

A detailed plan provides the process for recovery in the event of a failure. Your plan should include how to respond to a failure of both restaurant-level systems (such as the POS or payment networks) and any enterprise systems (such as payroll or email systems). Include points of contact for support and procedures to follow during the outage to ensure continuity of service. Test the plan each year and update it with lessons learned.

CRITICALITY
●●●●●

DIFFICULTY
●●●

PR.IP-11 Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)

How to apply in your restaurant:

- 1) Screen new hires to determine an individual's suitability for specific roles and identify any risk they may pose to information systems. This applies to both company hires and contract workers.
- 2) Conduct security training whenever there is a change in roles and responsibilities.
- 3) Follow appropriate procedures whenever there is a change in role and responsibilities to verify that the individual's access to information and systems is appropriate to their role and all access is revoked upon termination of their role.

Anticipated outcomes if action completed:

Ensure that security practices are followed whenever there are changes in personnel. Measures should include appropriate screening to determine an individual's suitability for specific roles, training on security practices and procedures, processes to verify that each individual's access to information and systems is appropriate to their role and responsibilities, and all access is revoked upon separation (company and contract workers).

CRITICALITY
●●●●●

DIFFICULTY
●●●

PR.IP-12 A vulnerability management plan is developed and implemented

How to apply in your restaurant:

- 1) Conduct vulnerability scans (internal and external systems) monthly to identify and classify known vulnerabilities.
- 2) Apply a repeatable approach to remediating identified vulnerabilities based on the severity and projected impact on your business.
- 3) Determine if a vulnerability is acceptable from a risk perspective; document the business justification.

Anticipated outcomes if action completed:

Review your IT assets at least monthly for known vulnerabilities. Include network and computer operating systems, all supported applications, internet browsers for internal assets and externally facing systems. Classify and remediate identified vulnerabilities within 30 days through the application of patches or updates.

CRITICALITY
●●●●●

DIFFICULTY
●●●

NIST CATEGORY: Maintenance (PR.MA)

Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.

PR.MA-1 Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools

How to apply in your restaurant:

- 1) Vet your IT equipment service providers to confirm that they have the required skills, toolsets, regulatory requirements and certifications to support your IT assets.
- 2) Remove from service any IT equipment that is not performing correctly until repairs can be completed.
- 3) Log the maintenance and repair of equipment to maintain a history of issues and changes made to individual IT components.

Anticipated outcomes if action completed:

Validate IT service providers for knowledge, tools and certifications appropriate for the supported IT assets. Maintain logs for individual IT assets that indicate issues and resolutions to identify potential indicators of compromise.

CRITICALITY



DIFFICULTY



PR.MA-2 Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access

How to apply in your restaurant:

- 1) Allow only preapproved, authorized vendors to repair IT equipment at remote locations.
- 2) Vendors working at remote locations should be clearly identified via a badge or uniform.

Anticipated outcomes if action completed:

Restaurants often use technicians to repair, replace or troubleshoot IT-related equipment, including POS, network and computer assets. Technicians should be preapproved for access to the location, whether physically or through remote connectivity, and provide proof of identity before they are given access to IT assets within the restaurant.

CRITICALITY



DIFFICULTY



NIST CATEGORY: Protective Technology (PR.PT)

Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.

PR.PT-1 Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

How to apply in your restaurant:

- 1) Collect security event logs from network devices, servers and endpoint devices.
- 2) Synchronize security event log data to ensure that event time is correlated across all devices.
- 3) Centralize the collection of security event log data from all devices.
- 4) Retain security event logs in accordance with policy. Check with PCI for the latest requirements for the PCI Data Security Standard.
- 5) Do not retain security event log data for periods longer than specified by policy.

Anticipated outcomes if action completed:

It is important to collect security event log data from devices such as servers, network devices and endpoints to ensure that events are captured for review and analysis. This provides a forensic trail to identify and determine the source of performance issues, breaches and attacks. Logs should be reviewed on a regular basis to identify variances from baseline behaviors. All log data should be collected and stored centrally to meet policy and compliance requirements for retention and review.

CRITICALITY



DIFFICULTY



Protective Technology (PR.PT) continued

PR.PT-2 Removable media is protected and its use restricted according to policy

How to apply in your restaurant:

- 1) Identify, label and monitor USB-connected devices for data leakage (unauthorized transfer of sensitive data). These include USB drives, phones, cameras or music players capable of storing external data.
- 2) Monitor or disable USB ports on servers and laptops according to your policy.
- 3) Clearly label external devices used for backups and store them according to policy during transport, storage and restore processes.

Anticipated outcomes if action completed:

Monitor removable media devices such as USB drives, external storage devices and external devices capable of storage for data leakage. Consider policies that restrict access or data transfer to external storage devices.

CRITICALITY



DIFFICULTY



PR.PT-3 Access to systems and assets is controlled, incorporating the principle of least functionality

How to apply in your restaurant:

- 1) Require individual user accounts for access to your systems. Never use shared accounts for access to applications or data.
- 2) Grant users the fewest privileges necessary to complete their job.
- 3) Log all access to systems, including invalid login attempts.
- 4) Require unique accounts for each user and log access to network devices, appliances and other managed devices.
- 5) Allow only authorized personnel to access physical locations such as offices or data centers that store assets.

Anticipated outcomes if action completed:

Require unique logins for every user of your IT devices, including network devices, servers, applications and connected devices. Grant the fewest privileges needed to perform defined job functions. Log user access to capture both successful and unsuccessful login attempts.

CRITICALITY



DIFFICULTY



PR.PT-4 Communications and control networks are protected

How to apply in your restaurant:

- 1) Limit access to network technologies such as MPLS, DSL and cable connections to authorized users and networks.
- 2) Limit access to networks used for the management of systems such as SNMP (Simple Network Management Protocol) and SSH (Secure Shell) to authorized users.

Anticipated outcomes if action completed:

Secure design, configuration and management of communication technologies is required to protect data in motion and data stored on either side of the connection. Securing these connections is most often a combination of systems such as firewalls and routers, and access controls such as management accounts. Protocols used to manage networks should remove default logons and require individual, logged access for all activities.

CRITICALITY



DIFFICULTY



NIST CATEGORY: Anomalies and Events (DE.AE)

Anomalous activity is detected in a timely manner and the potential impact of events is understood.

DE.AE-1 A baseline of network operations and expected data flows for users and systems is established and managed

How to apply in your restaurant:

- 1) Establish baseline configurations for information systems and system components, including communications and connectivity-related aspects of systems.
- 2) Document system configurations for all computers and network devices and use them for all new deployments.

Anticipated outcomes if action completed:

Maintain baseline configurations to ensure documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items within those systems.

CRITICALITY



DIFFICULTY



DE.AE-2 Detected events are analyzed to understand attack targets and methods

How to apply in your restaurant:

- 1) Configure alert systems to identify security-related attacks and alert a designated individual/team or vendor.
- 2) Review daily systems that send alerts such as virus and network security tools.

Anticipated outcomes if action completed:

Use alerts to trigger an investigation and security response if necessary.

CRITICALITY



DIFFICULTY



DE.AE-3 Event data are aggregated and correlated from multiple sources and sensors

How to apply in your restaurant:

- 1) Use security information and event management (SIEM) tools to aggregate your audit records and consolidate multiple information system components, including file integrity monitoring (FIM), antivirus (AV) attacks, intrusion prevention systems (IPS) and rogue hardware detection.

Anticipated outcomes if action completed:

Store audit records for security-related events in an easily accessible area in case they are needed for investigations.

CRITICALITY



DIFFICULTY



DE.AE-4 Impact of events is determined

How to apply in your restaurant:

- 1) Prepare, maintain and test plans that document the specific steps to take when a risk event may seriously impact your business.
- 2) Train your response team to properly document and respond to all risk events.

Anticipated outcomes if action completed:

Develop contingency plans to restore information systems and implement alternative mission/business processes when systems are compromised.

CRITICALITY



DIFFICULTY



DE.AE-5 Incident alert thresholds are established

How to apply in your restaurant:

- 1) Respond in a timely manner with effective measures to limit the magnitude of loss from IT-related events.
- 2) Categorize incidents and compare actual exposures against risk-tolerance thresholds.
- 3) Apply the appropriate response plan to minimize the impact when risk incidents occur.

Anticipated outcomes if action completed:

Recognize that incident response capability is dependent on the capabilities of organizational information systems and the mission/business supported by those systems. Communicate business impacts to decision-makers as part of reporting, and update your risk profile. Examine past adverse events/losses and missed opportunities to determine root causes. Communicate those root causes, additional risk-response requirements and process improvements to appropriate decision-makers and include them in your risk-governance processes.

CRITICALITY



DIFFICULTY



NIST CATEGORY: Security Continuous Monitoring (DE.CM)

The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

DE.CM-1 The network is monitored to detect potential cybersecurity events

How to apply in your restaurant:

- 1) Monitor your network to detect potential cybersecurity events. Segment the network based on the label or classification level of the information stored on the servers.
- 2) Review all user accounts and disable those that are no longer being used or are no longer associated with a business process.
- 3) Encrypt sensitive stored information and require a secondary authentication mechanism, not integrated into the operating system, in order to access the information.

Anticipated outcomes if action completed:

Protect all information stored on systems with file system, network share, claims application or database-specific access control lists. Only authorized individuals should have access to the information based on their responsibilities. Monitor account usage to determine dormant accounts, notifying the user or user's manager. Disable such accounts if not needed, or document and monitor exceptions (e.g., vendor maintenance accounts needed for system recovery or continuity operations). Require that managers match active employees and contractors with each account belonging to their managed staff. Security or system administrators should then disable accounts that are not assigned to valid workforce members. Ensure that all account user names and authentication credentials are transmitted across networks via encrypted channels.

CRITICALITY



DIFFICULTY



DE.CM-2 The physical environment is monitored to detect potential cybersecurity events

How to apply in your restaurant:

- 1) Develop a continuous monitoring strategy and implement a continuous monitoring program.
- 2) Establish physical access controls for both your information systems and your facility.

Anticipated outcomes if action completed:

Assess/analyze security controls and information security risks at a frequency sufficient to support organizational risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Also, this control provides additional security for those areas where there is a concentration of information systems components (such as server rooms, media storage areas, and data and communications centers).

CRITICALITY



DIFFICULTY



DE.CM-3 Personnel activity is monitored to detect potential cybersecurity events

How to apply in your restaurant:

- 1) Record user activities, exceptions, faults and information security events in a log, and regularly review the logs.
- 2) Establish and administer privileged user accounts in accordance with role-based access. Monitor privileged role assignments and remove access when a role assignment is no longer appropriate.

Anticipated outcomes if action completed:

Identify authorized users of your information systems and place controls on their access privileges. Automatically remove both temporary and emergency accounts after a predefined period of time has elapsed, rather than at the convenience of the systems administrator. Privileged roles are organization-defined roles that allow assigned individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These roles include key management, account management, network and system administration, database administration and web management.

CRITICALITY



DIFFICULTY



Security Continuous Monitoring (DE.CM) continued

DE.CM-4	Malicious code is detected	<p><i>How to apply in your restaurant:</i> Use malware detection tools to detect malicious code and alert security personnel.</p>	<p><i>Anticipated outcomes if action completed:</i> Quarantine and neutralize malicious code. Isolate, clean and put back into service workstations and endpoints infected by the attack. Determine infiltration methods and consider adjustments to defenses.</p>	<p>CRITICALITY ●●●●●</p> <p>DIFFICULTY ●●●</p>
DE.CM-5	Unauthorized mobile code is detected	<p><i>How to apply in your restaurant:</i> Use malware detection tools to detect unauthorized code on mobile devices, and alert security personnel.</p>	<p><i>Anticipated outcomes if action completed:</i> Determine the severity of unauthorized code and the appropriate next steps. Note that the line between business and personal applications on mobile devices is difficult to manage. A mobile device management (MDM) solution will greatly improve separation and management of apps and data on mobile devices.</p>	<p>CRITICALITY ●●●●●</p> <p>DIFFICULTY ●●●</p>
DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events	<p><i>How to apply in your restaurant:</i> Monitor contractor access and credentials to your company’s network, applications and data — both at your place of business and remotely.</p>	<p><i>Anticipated outcomes if action completed:</i> Log and review external service provider activity to ensure that use of your computer assets satisfies your company’s Acceptable Use Policy (AUP) and meets your criteria for system use and data access.</p>	<p>CRITICALITY ●●●●●</p> <p>DIFFICULTY ●●●</p>
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	<p><i>How to apply in your restaurant:</i> Monitor and detect foreign devices on credit terminals. If unauthorized devices, connections or software are detected, remove the credit terminals from the network and stop taking credit.</p>	<p><i>Anticipated outcomes if action completed:</i> The security incident is contained and the information is available for a security review (forensics).</p>	<p>CRITICALITY ●●●●●</p> <p>DIFFICULTY ●●●</p>
DE.CM-8	Vulnerability scans are performed	<p><i>How to apply in your restaurant:</i> Perform scans to detect medium-to-low risk and high-risk vulnerabilities to the system.</p>	<p><i>Anticipated outcomes if action completed:</i> Based on your organization’s risk tolerance, determine the impact of a fix and apply it if necessary. If a fix cannot be applied right away, attempt to mitigate the vulnerability and monitor it closely. Consider taking the system down if the risk is high enough.</p>	<p>CRITICALITY ●●●●●</p> <p>DIFFICULTY ●●●</p>

NIST CATEGORY: Detection Processes (DE.DP)

Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

DE.DP-1 Roles and responsibilities for detection are well defined to ensure accountability

How to apply in your restaurant:

- 1) Install a malware detection system for your organization.
- 2) Define the process for how users will report potentially malicious activity. Potentially malicious emails should be referred to an incident-response team.

Anticipated outcomes if action completed:

Establish a process for maintaining and monitoring the system, and define who will be responsible for keeping the system up to date and healthy. Who will be responsible for monitoring the alerts and logs from the system? How will this fit into your incident response process? Users should understand their roles and responsibilities and be able to detect potentially malicious email.

CRITICALITY



DIFFICULTY



DE.DP-2 Detection activities comply with all applicable requirements

How to apply in your restaurant:

- 1) Develop and implement a detection process.
- 2) Establish a process for monitoring regulatory bodies that publish requirements such as PCI, HIPAA, state/federal laws, etc.
- 3) Develop a detection process that meets compliance requirements.
- 4) Implement the process and test it to make sure it complies.

Anticipated outcomes if action completed:

Keep up with new compliance requirements and detection standards (such as PCI, HIPAA, state/federal laws). Your detection activities should comply with applicable requirements.

CRITICALITY



DIFFICULTY



DE.DP-3 Detection processes are tested

How to apply in your restaurant:

Have a trained security administrator periodically test your defenses. Vary your testing methods and times.

Anticipated outcomes if action completed:

If your defenses are working properly, attempts to penetrate your network will be blocked. If this is not the case, remedy the situation and test again.

CRITICALITY



DIFFICULTY



DE.DP-4 Event detection information is communicated to appropriate parties

How to apply in your restaurant:

As part of an information security risk plan, document how you plan to communicate a security event.

Anticipated outcomes if action completed:

The level of the communication is dependent on the severity of the detected event. For example, a credit card breach should be communicated to the highest levels of your organization.

CRITICALITY



DIFFICULTY



DE.DP-5 Detection processes are continuously improved

How to apply in your restaurant:

- 1) Upgrade your software and firmware so you are using the latest releases.
- 2) Review your detection systems at least annually to ensure that your security needs are being met.

Anticipated outcomes if action completed:

Keep security solutions current to detect evolving threat actors and mitigate vulnerabilities.

CRITICALITY



DIFFICULTY



NIST CATEGORY: Response Planning (RS.RP)

Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.

RS.RP-1 Response plan is executed during or after an event

How to apply in your restaurant:

Develop and follow a response plan, even for low-level events, to better prepare your team for high-level incidents.

Anticipated outcomes if action completed:

If you have a plan in place, the effects of cybercrime will be shorter, your response will be more organized, and your external and internal customers are likely to be more satisfied that you are taking the necessary steps to resolve the breach.

CRITICALITY



DIFFICULTY



NIST CATEGORY: Communications (RS.CO)

Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.

RS.CO-1 Personnel know their roles and order of operations when a response is needed

How to apply in your restaurant:

Notify your security team and managers when an event occurs. Ensure that your team knows their roles and how to respond.

Anticipated outcomes if action completed:

During a security event, all personnel will know their roles, and the response plan will be implemented quickly.

CRITICALITY



DIFFICULTY



RS.CO-2 Events are reported consistent with established plan

How to apply in your restaurant:

Have a plan in place that spells out what needs to be communicated, and to whom, when an event occurs.

Anticipated outcomes if action completed:

The correct people in and outside your organization are informed.

CRITICALITY



DIFFICULTY



RS.CO-3 Information is shared consistent with response plans

How to apply in your restaurant:

Develop a crisis communications plan, and follow it during an incident. Share the information needed to properly respond.

Anticipated outcomes if action completed:

Appropriate stakeholders (vendors, customers, etc.) will stay updated and information needed for recovery will be shared with your partners.

CRITICALITY



DIFFICULTY



RS.CO-4 Coordination with stakeholders occurs consistent with response plan

How to apply in your restaurant:

Consistently update your stakeholders so they can help reduce the impact of an incident.

Anticipated outcomes if action completed:

Your entire team should be working on solving the problem and keeping your restaurant functional.

CRITICALITY



DIFFICULTY



RS.CO-5 Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness

How to apply in your restaurant:

Periodically share risk trends and security information with stakeholders.

Anticipated outcomes if action completed:

Full awareness of a security risk will lessen the risk.

CRITICALITY



DIFFICULTY



NIST CATEGORY: Analysis (RS.AN)

Analysis is conducted to ensure adequate response and support recovery activities.

RS.AN-1 Notifications from detection systems are investigated

How to apply in your restaurant:

Review alerts immediately with your personnel/vendors from any systems that send alerts, such as virus and network-security tools.

Anticipated outcomes if action completed:

Your team should respond to any unusual alerts. Investing in tools or partnerships that enhance your monitoring capabilities will make this task less difficult.

CRITICALITY



DIFFICULTY



RS.AN-2 The impact of the incident is understood

How to apply in your restaurant:

Understand that as an event begins, your first discoveries may not be the source of the problem. As an example, one person skimming in a restaurant may lead to your finding that others are involved. Or you may find that one breached system leads to another breached system.

Anticipated outcomes if action completed:

You need to know the extent of the entire problem so you can fully resolve it.

CRITICALITY



DIFFICULTY



RS.AN-3 Forensics are performed

How to apply in your restaurant:

In the event of a major breach of your systems, perform a forensics audit. Consult immediately with a forensics expert to ensure that you are properly maintaining evidence and can mitigate the breach as soon as possible.

Anticipated outcomes if action completed:

You will understand fully what happened in the incident and know when it is resolved.

CRITICALITY



DIFFICULTY



RS.AN-4 Incidents are categorized consistent with response plans

How to apply in your restaurant:

Follow your response plan to ensure clear thinking and that appropriate actions are taken.

Anticipated outcomes if action completed:

Following your response plan ensures that you correctly respond to an event.

CRITICALITY



DIFFICULTY



NIST CATEGORY: Mitigation (RS.MI)

Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.

RS.MI-1 Incidents are contained

How to apply in your restaurant:

Contain incidents to lessen their impact on your restaurant. For example, if a foreign device is detected on a credit terminal, remove the credit terminals at that location and stop taking credit.

Anticipated outcomes if action completed:

Contain incidents and safeguard any information needed for a security review (forensics).

CRITICALITY



DIFFICULTY



RS.MI-2 Incidents are mitigated

How to apply in your restaurant:

Collect evidence concerning the incident, and follow your response plan to mitigate or eliminate the incident. In the event of a foreign device on a credit terminal, stop taking credit, take it off the network, secure the device and check all other devices. Bring in known good replacement devices to replace the suspected devices. Store the infected device somewhere that is secured. It may become legal evidence and should not be tampered with.

Anticipated outcomes if action completed:

Your operations will be temporarily impacted by most incidents, but you must ensure the security of your customers' and team's data. The goal is to eliminate the incident and restore operations as soon as they can be secured.

CRITICALITY



DIFFICULTY



Mitigation (RS.MI) continued

RS.MI-3 Newly identified vulnerabilities are mitigated or documented as accepted risks

How to apply in your restaurant:

Apply your learning from evidence collection and perform any migration/corrective tasks.

Anticipated outcomes if action completed:

Your operation will be able to resume in a secured and safe manner. Your team will be better trained to prevent this in the future.

CRITICALITY



DIFFICULTY



NIST CATEGORY: Improvements (RS.IM)

Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

RS.IM-1 Response plans incorporate lessons learned

How to apply in your restaurant:

Having a meeting after every incident to discuss lessons learned.

Anticipated outcomes if action completed:

An evolving plan that improves with time will reduce the likelihood and impact of a similar event.

CRITICALITY



DIFFICULTY



RS.IM-2 Response strategies are updated

How to apply in your restaurant:

Learning how to respond starts with a plan rather than the experience itself. Always update your plans.

Anticipated outcomes if action completed:

Incorporate into your plan the experience you've gained from each response to an incident.

CRITICALITY



DIFFICULTY



NIST CATEGORY: Recovery Planning (RC.RP)

Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.

RC.RP-1 Recovery plan is executed during or after an event

How to apply in your restaurant:

Carry out your recovery plan to limit the impact of your event.

Anticipated outcomes if action completed:

In a crisis, strong partnerships and a strong plan are the keys to your recovery.

CRITICALITY



DIFFICULTY



NIST CATEGORY: Improvements (RC.IM)

Recovery planning and processes are improved by incorporating lessons learned into future activities.

RC.IM-1 Recovery plans incorporate lessons learned

How to apply in your restaurant:

Your recovery plan should incorporate lessons learned from responding to the incident. For example, if an employee was skimming cards at your restaurant, review with your team how they handled the incident and what improvements can be made to your practices.

Anticipated outcomes if action completed:

Your response plan evolves and becomes stronger over time.

CRITICALITY



DIFFICULTY



Improvements (RC.IM) continued

RC.IM-2 Recovery strategies are updated

How to apply in your restaurant:

Learn from real security incidents, and use those lessons to update your response plan. Annually review your plan with your security team or vendor partners.

Anticipated outcomes if action completed:

Recognize that your response plan is an evolving document that grows with your business and adapts to new threats. Apply the lessons you have learned so you don't repeat past mistakes.

CRITICALITY



DIFFICULTY



NIST CATEGORY: Communications (RC.CO)

Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

RC.CO-1 Public relations are managed

How to apply in your restaurant:

Implement a crisis communications plan to manage the public relations fallout from the incident. Consider hiring an outside PR consultant to help you.

Anticipated outcomes if action completed:

Customers fully understand that you are doing everything you can to mitigate the event.

CRITICALITY



DIFFICULTY



RC.CO-2 Reputation after an event is repaired

How to apply in your restaurant:

Take steps to repair your reputation after a security incident. For example, if email addresses are the only information that is breached, assure your customers that no other personal information was compromised. Be very clear in your communications to avoid misunderstandings. Do not forget to apologize and note that you are taking steps to ensure that this will not happen again. Work with PR partners when available.

Anticipated outcomes if action completed:

A fully informed customer will remain a customer.

CRITICALITY



DIFFICULTY



RC.CO-3 Recovery activities are communicated to internal stakeholders and executive and management teams

How to apply in your restaurant:

Keep managing partners, owners and other key stakeholders informed of your recovery process. For example, if a loyalty program was compromised and you have shut down this system, you should continue to communicate and give daily updates to your internal team.

Anticipated outcomes if action completed:

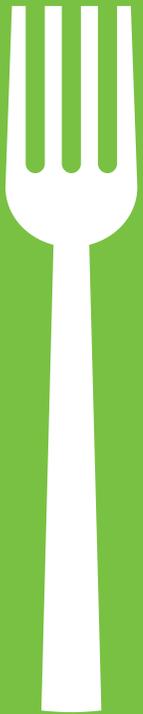
Keep all team members informed, so they can do what is best in their operational area to assure customer satisfaction.

CRITICALITY



DIFFICULTY





At a Glance: What’s Urgent

Not sure where to start? Within the NIST Cybersecurity Framework’s five core functions/areas (**Identify, Protect, Detect, Respond** and **Recover**), the Framework offers nearly 100 subcategories for companies to consider. In Section 2 of this report, we include detailed overviews of all the subcategories, including the importance/difficulty ratings our team of restaurant cybersecurity experts assigned to each subcategory.

As you plan, you may want to begin with the items our team has rated as **Urgent** (noted as ●●●● in Section 2, denoting the highest level of importance). We’ve highlighted the **Urgent** items in the Appendix, for an “at a glance” look. We have also given you some questions to ask as you work your way through each **Urgent** item, along with potential outcomes you can expect as you complete these.

Note: The items rated Urgent are a subset of a more comprehensive set of security steps. Implementation does not guarantee that your business will not experience a data breach. We encourage you to consult with cybersecurity experts as you develop your plans.

Identify

 **ID.AM-3 Organizational communication and data flows are mapped**

Questions to ask:

Has someone with IT experience diagrammed how information moves in your operation? For example, credit card information moves from POS device to server to processor, etc. Has an IT expert drafted network diagrams? Have these been updated? Who has access to them?

Anticipated outcomes if action completed:

Your operation should prepare and periodically update a document describing the information flow within the business and how IT software, hardware and personnel support that information flow. The document should describe how this information supports your business objective and describe the relative risk to the business.

 **ID.BE-4 Dependencies and critical functions for delivery of critical services are established**

Questions to ask:

Have you created a list of services that are critical to running your business? Do you understand and have you documented all of the technologies, vendor partners or service providers that are required to deliver these services? Do you understand the consequences if these services are not available? Do you have a backup plan?

Anticipated outcomes if action completed:

You and your staff understand what critical services are needed to run your business and what key functions are needed to provide those services.

 **ID.GV-3 Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed**

Questions to ask:

Does the person (and/or your managed service provider) responsible for overseeing the IT function in your restaurant keep up with changing industry standards and regulatory requirements? Are you given updates? Do you review these updates with senior managers to determine if additional controls are needed?

Anticipated outcomes if action completed:

The organization should be mindful of the constantly changing legal environment and industry standards related to cybersecurity. Subject matter experts must communicate and inform the organization of changes that impact the business and allow management to assess risk tolerance and determine if additional controls should be implemented.

**ID.RA-3****Threats, both internal and external, are identified and documented****Questions to ask:**

Have you identified threats to your business, both internally and externally? Have you created a structure for gathering, consolidating and documenting this information? Have you used resources provided by the National Restaurant Association or other industry sources? (Contact the NRA's membership department to learn more about our resources.)

Anticipated outcomes if action completed:

Develop a list of threats to your operation and update them on a regular basis. This covers all threats, including outside and within the organization, those of a technical nature and those of a human nature. You do not need to consider the actual risk or impact associated with these threats — that will be addressed by other elements of the overall risk assessment strategy.

**ID.RM-1****Risk management processes are established, managed and agreed to by organizational stakeholders****Questions to ask:**

Do you have a procedure for periodically reviewing your risks? Who is included in your risk-assessment reviews? Do you document these reviews?

Anticipated outcomes if action completed:

Establish a risk-assessment process with regular reviews by key members of your organization.

Protect

**PR.AC-3****Remote access is managed****Questions to ask:**

Are you managing remote access to your systems? Do you require third-party providers to use unique, individual logins? Are you managing third-party data connectivity? Are you limiting third-party access to only those systems that need to be accessed? Do you keep a log of who is accessing your system?

Anticipated outcomes if action completed:

Remote access includes internal business connections, service providers and third-party data connections. All of these connections are required to have unique credentials for each user with access. All access should be limited to only the hardware, applications or data required. All activities performed remotely should be logged. All access to the Payment Card Industry (PCI) cardholder data network should require two-factor authentication.

**PR.AC-4****Access permissions are managed, incorporating the principles of least privilege and separation of duties****Questions to ask:**

Have you granted administrative status to the fewest users possible? Do user permissions correspond to job functions? Are privileges limited to the fewest necessary to perform the job?

Anticipated outcomes if action completed:

Manage and document the roles and level of access for each individual user with access to your systems. Closely guard administrative and super-user accounts and only share them with trusted employees. Provide the least amount of access required to perform a job. Segregate duties to separate development and testing from production.

**PR.AC-5****Network integrity is protected, incorporating network segregation where appropriate****Questions to ask:**

Are critical systems and applications separated by virtual or physical firewalls? Are wireless networks on separate networks to enhance security? Do you use VLANs (virtual Local Area Networks) or VRFs (virtual routing and forwarding) to separate applications at the network layer?

Anticipated outcomes if action completed:

Access to all networks, both wired and wireless, should be secured through the implementation of physical firewalls. Technologies such as a stateful firewall (a network firewall that tracks the operating state and characteristics of network connections conversing it) can also be used to segregate network traffic for critical applications. Firewalls make it more difficult for breaches to spread across network infrastructure and for adversaries to export compromised data.

PR.AT-5 Physical and information security personnel understand roles and responsibilities

Questions to ask:

Have you documented procedures for security practices and daily operational processes? Do you have guidelines for granting permission to other users? Are you providing appropriate security training?

Anticipated outcomes if action completed:

Security personnel have the right to change both user permissions and security settings/configurations. Due to this advanced level of access, it is imperative that these personnel are selected carefully and provided an appropriate level of training and review. Any mistake at this level can be critical.

PR.PT-4 Communications and control networks are protected

Questions to ask:

Have you secured network technologies to limit access to only authorized users and networks? Do you allow only authorized users to access networks?

Anticipated outcomes if action completed:

Secure design, configuration and management of communication technologies is required to protect data in motion and data stored on either side of the connection. Securing these connections is most often a combination of systems such as firewalls and routers, and access controls such as management accounts. Protocols used to manage networks should remove default logons as well as require individual, logged access for all activities.

Detect

DE.CM-1 The physical environment is monitored to detect potential cybersecurity events

Questions to ask:

Are you monitoring your network to detect potential cybersecurity events? Are you segmenting your networks based on the classification levels of stored information? Are you reviewing user accounts and disabling those that are no longer being used or associated with a business process? Do you encrypt sensitive stored information and require a secondary authentication mechanism to access it?

Anticipated outcomes if action completed:

Protect all information stored on systems with file system, network share, claims application or database-specific access control lists. Only authorized individuals should have access to the information. Monitor account usage to determine dormant accounts and notify the user or user's manager. Disable such accounts if not needed, or document and monitor exceptions (e.g., vendor maintenance accounts needed for system recovery or continuity operations). Require that managers match active employees and contractors with each account belonging to their staff. Security or system administrators should then disable accounts not assigned to valid workforce members. Ensure that all account user names and authentication credentials are transmitted across networks via encrypted channels.

DE.CM-4 Malicious code is detected

Questions to ask:

Are you using malware tools to detect malicious code and alert security personnel?

Anticipated outcomes if action completed:

Quarantine and neutralize malicious code. Isolate, clean and put back into service workstations and end points infected by the attack. Determine infiltration methods and consider adjustments to defenses.

Respond



RS.RP-1 Response plan is executed during or after an event

Questions to ask:

Do you have a response plan and are you following it?

Anticipated outcomes if action completed:

If you have a plan in place, the effects of cybercrime will be shorter, your response will be more organized, and your external and internal customers are likely to be more satisfied that you are taking the necessary steps to resolve the breach.



RS.CO-3 Information is shared consistent with response plans

Questions to ask:

Do you have a crisis communications plan? If so, are you following it? Are you sharing the information needed to properly respond to the crisis?

Anticipated outcomes if action completed:

Appropriate stakeholders (vendors, customers, etc.) will stay updated and information needed for recovery will be shared with your partners.



RS.CO-4 Coordination with stakeholders occurs consistent with response plan

Questions to ask:

Have you consistently updated your stakeholders so they can help you reduce the impact of the incident?

Anticipated outcomes if action completed:

Your entire team should be working on solving the problem and keeping your restaurant functional.



RS.AN-2 The impact of the incident is understood

Questions to ask:

Do you fully understand the impact of the incident? Have you investigated to see how extensive the incident is?

Anticipated outcomes if action completed:

You need to know the extent of the entire problem so you can fully resolve it.

Recover



RS.CO-1 Public relations are managed

Questions to ask:

Are you managing the public relations fallout from the incident?

Anticipated outcomes if action completed:

Customers fully understand that you are doing everything you can to mitigate the event.

Glossary

BACKUP – The copying of physical or virtual files or databases to a secondary site for preservation in case of equipment failure or other catastrophe. (WhatIs.com)

CYBER FORENSICS – The application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. (WhatIs.com)

DATA AT REST – Data in computer storage, excluding data that is in motion or temporarily residing in computer memory to be read or updated. (WhatIs.com)

DATA EXFILTRATION (OR EXTRUSION) – The unauthorized transfer of data from a computer. Such a transfer may be manual and carried out by someone with physical access to a computer, or it may be automated and carried out through malicious programming over a network. (WhatIs.com)

DATA IN TRANSIT (OR MOTION) – Data that flows over a public or untrusted network, or data that flows over a private network or local area network. (Wikipedia)

DATA LEAKAGE – The unauthorized transfer of information from a computer or data center to the outside world. (PC Encyclopedia)

ENCRYPTION – The conversion of electronic data into another form, called ciphertext, which cannot be easily understood by anyone except authorized parties. (WhatIs.com)

FIREWALL – A network security system, either hardware- or software-based, that uses rules to control incoming and outgoing network traffic. A firewall acts as a barrier between a trusted network and an untrusted network. (WhatIs.com)

FIRMWARE – Programming that's written to the read-only memory of a computing device. Firmware, which is added at the time of manufacturing, is used to run user programs on the device. (WhatIs.com)

MALWARE (MALICIOUS SOFTWARE) – Any program or file that is harmful to a computer user. Malware includes computer viruses, worms, Trojan horses and spyware. (WhatIs.com)

NETWORK – A group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users. (Techopedia)

NIST CYBERSECURITY FRAMEWORK – Created through collaboration between industry and government, the voluntary Framework consists of standards, guidelines and practices to promote the protection of critical infrastructure. (National Institute of Standards and Technology)

PATCH (FIX) – A quick-repair job for a piece of programming to fix bugs. A patch is the immediate solution that is provided to users; it can sometimes be downloaded from the software maker's website. (WhatIs.com)

PCI – The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment. (PCIComplianceGuide.org)

PERSONALLY IDENTIFIABLE INFORMATION (PII) – Any data that could potentially identify a specific individual. (WhatIs.com)

PHISHING – A form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email, instant messaging or other communication channels. (WhatIs.com)

SPAM – Unsolicited or undesired electronic messages. (Wikipedia)

THREAT ACTOR – An entity that is partially or wholly responsible for an incident that impacts — or has the potential to impact — an organization's security. (WhatIs.com)

TWO-FACTOR AUTHENTICATION (2FA) – A security process in which the user provides two authentication factors to verify they are who they say they are. (WhatIs.com)

USER ACCOUNT – An established relationship between a user and a computer, network or information service. User accounts are assigned a username and usually a password. (PCMag Encyclopedia)

VIRUS – Malicious code that replicates by copying itself to another program, computer boot sector or document and changes how a computer works. (WhatIs.com)

VULNERABILITY – A flaw in code or design that creates a potential point of security compromise for an endpoint or network. (WhatIs.com)

WHITELIST – A list of email addresses or domain names from which an email blocking program will allow messages to be received. (WhatIs.com)

Keeping Payment Data Safe

The Payment Card Industry Data Security Standard and the NIST Framework

Every entity responsible for the security of payment card data — including restaurants that accept credit and debit cards — is responsible for following the Payment Card Industry Data Security Standard.

What’s the PCI Data Security Standard?

The PCI DSS aims to protect the security of payment card data. The PCI DSS outlines a set of security requirements (see box below) that companies must follow if they accept, process, store or transmit payment card data. It applies regardless of the size or number of transactions, and applies to any entity that accepts, transmits or stores any cardholder data.

The PCI DSS is administered and managed by the PCI Security Standards Council, which was formed by the major payment card brands (Visa, MasterCard, American Express, Discover and JCB). The PCI Council does not enforce compliance. Payment brands and acquiring/merchant banks are responsible for making sure restaurants and any other merchants that accept payment cards are compliant with the PCI DSS.

What’s the difference between the PCI DSS and the NIST Cybersecurity Framework?

It’s important to realize that the PCI DSS and NIST Cybersecurity Framework are two entirely different things.

The PCI DSS is a comprehensive set of requirements that any company that accepts payment cards must follow in order to ensure payment card data remains protected and secure. The major payment card brands

formed the PCI Security Standards Council that administers and updates the PCI DSS. The card brands and acquiring/merchant banks enforce the standard.

The NIST Cybersecurity Framework, on the other hand, is not a requirement. It doesn’t specify a set of tasks to be completed. Instead, it’s a way of thinking about managing cybersecurity risks across your organization. It provides an approach to cybersecurity in general. It’s not limited to protecting a particular set of data, such as payment card data.

Will I be protected from a payment-card data breach if I follow the PCI DSS and NIST Cybersecurity Framework?

Unfortunately, there are no 100 percent guarantees that you won’t experience a breach of payment card data. The PCI DSS requires you to complete specific tasks to protect payment card data. However, these specific tasks may not be successful in stopping all payment-card data breaches.

Using the NIST Cybersecurity Framework to guide your cybersecurity planning also doesn’t guarantee that you won’t face a breach of payment-card or any other data. The NIST Framework is a guide and way of thinking about how you can manage the risk or likelihood of a data breach.

PCI Security Standards: If you accept or process payment cards, the PCI Data Security Standards apply to you. These standards cover technical and operational system components included in or connected to cardholder data.

GOALS	PCI DSS REQUIREMENTS
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a policy that addresses information security for employees and contractors

Source: PCI Security Standards Council

WHAT COMES NEXT?

As the National Institute of Standards and Technology continues to improve and update its Cybersecurity Framework, the National Restaurant Association will keep our members informed. Check Restaurant.org/Cybersecurity for the latest information.

The National Restaurant Association will also continue to work to shape effective public policy on data security and breach-notification laws. State-level regulators and legislators are already involved in data security issues, and Congress is likely to weigh in as well. The NRA is working to ensure that Congress avoids regulatory overreach when it comes to data security.

Resources

- National Institute of Standards and Technology (NIST) - [Cybersecurity Framework](#)
- Federal Trade Commission - [Data Security](#)
- Department of Homeland Security - [Cybersecurity](#)
- Internet Crime Complaint Center (a partnership between the FBI and the National White Collar Crime Center) - ic3.go



[Restaurant.org/Cybersecurity](https://www.restaurant.org/Cybersecurity)