

Digital Security 201

A Step-by-Step Guide to **PROTECTING**

RESTAURANT DATA



00 4567632211113004004<mark>0</mark>040 66707 0010123 E54677800 G7G880010167 0 645554G300<mark>1</mark>0 01101U009769644 004

> UPDATED: OCTOBER 2021 RESTAURANT.ORG/CYBERSECURITY

> > Sponsored by



About This Guide

As a restaurant operator, you routinely safeguard things of value to the 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, preparing, and serving food. 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.

Digital security has become crucial to a restaurant operation's success. Although digital, security may seem like an overwhelming issue, there's a lot you can do to protect your operations against data breaches—and those security measures don't have to be complicated, require special skills or cost a lot. Creating a digital security plan starts with some basic, straightforward steps.

The National Restaurant Association's "*Digital Security 101: The Basics of Protecting Your Restaurant's Data,*" guide highlights the National Institute of Standards and Technology (NIST) 5 core "functions" (areas) of digital security planning: Identify, Protect, Detect, Respond and Recover.

"DIGITAL SECURITY 201, A Step-by-Step Guide to Protecting Restaurant Data" builds on our original 2017 guide (Cybersecurity 201) to provide restaurant-specific security steps—rated by urgency—and is updated and edited to include the relevant changes and additions to the NIST <u>Data Security Framework 1.1</u> (2018).

We are grateful to the members of the National Restaurant Association's Information Technology Expert Exchange who generously devoted time and expertise to create the original and to help update this guide.

October 2021

Legal Disclaimer: The information provided here is a service to help guide your company's data security 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 data security experts when developing your data security plans.



© 2021 National Restaurant Association. All rights reserved. The National Restaurant Association logo is a registered trademark of the National Restaurant Association.

TABLE OF CONTENTS

INTRODUCTION1
CASE STUDIES • Security Scenarios: This Could Be You 2
A PLANNED APPROACH 8
DATA SECURITY FRAMEWORK 9
FIRST THINGS FIRST: WHAT'S URGENT?
THE NIST 1.1 CYBERSECURITY FRAMEWORK FOR RESTAURANTS 16

APPENDICE - Keeping Data Payment Safe 46



OUR MISSION

To serve the restaurant industry and impact its success, we:

• Strengthen operations, mitigate risk and develop talent

• Advance and protect business vitality through national, state and local advocacy

Drive knowledge and collaboration

Cybercrime: An Insidious 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 <u>Digital Security 101</u> 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—through card payments, payroll and human resources records, inventory control, or loyalty programs—online criminals and hackers can be waiting to attack where your operation is most vulnerable.

Statistics are sobering. A 2019 <u>survey</u> of decision-makers at small to medium size businesses (SMBs) revealed that 62% of those companies between \$1M and \$500M in revenue didn't believe a cyberattack was likely; that percentage rose to 73% among companies smaller than \$1M in revenue. In reality, 67% of SMBs experienced a cyberattack in the past year. Worse, the cost of these attacks to businesses keeps growing.

According to IBM's latest research, "Cost of a Data Breach 2021," companies spent an average of \$4.24M per incident, a 10% increase from the prior year, and the most in the 17 years that IBM has been releasing the report.



Doing something is better than nothing

The good news is that you can do something about it. 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.

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 accountant investigator to find out what happened. Those costs can range from \$10K to more than \$100K per investigation, depending on the size, complexity and extent of the breach.
- **REMEDIATION.** Depending on what the forensic accounting 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 a challenge.



SECURITY SCENARIOS This Could Be You

Check out five case studies that illustrate just how easily your operation's digital security could be compromised.



Karen

RANSOMWARE NIGHTMARE



Cheryl

NETWORK SECURITY SLIP-UP



Bruce

CLOUD-JACKING HOLDUP



Terri

DATA BREACH LIABILITY



Sam

PAYMENT CARDS COMPROMISED



Karen is the marketing manager for an 80-unit fast-casual chain who faced a deadline to launch a new menu promotion. But with four new restaurant openings coming up, she was pressed for time. When she received an email asking her company to participate in "Restaurant Week," she thought she had the perfect answer. She clicked on the email and unwittingly launched a cyberattack on the company.

The downloaded ransomware spread through the network, freezing access to all inventory, management, and production systems. An on-screen message said the system was hacked and that all proprietary information had been seized. The message said the hackers would release control of the information for thousands of dollars in Bitcoin.

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. The staff couldn't honor reservations, and the loyalty program was inaccessible. When the system was back up, the company discovered much of its data was lost. The consultant told them that unless they paid the ransom, they'd likely never recover it.

Using the NIST Framework, the company could have increased security measures, including employee digital security training , running weekly system scans for malware, backing up critical data in a secure location, installing security patches on all systems as soon as they're available, and tightening spam filters on the email system.



Cheryl is in the accounting department of a 500-unit regional quickservice chain. She has worked remotely from her home since the pandemic began and hasn't been to the office since. Both she and the company like the arrangement, and the company considers her a valuable employee.

She receives an email from the HR department saying it's reviewing its insurance providers and as a result is updating all employee records. Though she was usually wary about handing out personal information to just anyone, especially online, she is familiar with the sender's name, and the email appeared legitimate in every way. She sees no reason not to confirm her Social Security number and other personal information.

Several weeks later, while reviewing her credit card account, Cheryl notices that her credit score has changed. When she investigates further, she learns that someone has used her Social Security number to open a new credit card account. She later discovers that the email from her company's HR department had been a deep fake.

A hacker, piggybacking on her home Wi-Fi network, had broken into the company's network, stolen a list of company employees, and sent out the fake email. Nearly 50 employees had responded to the email before the company caught on, inadvertently giving the hacker personal information that it sold on the Dark Web.

Cheryl never thought to change the password on her home Wi-Fi network, and the company had no protocols in place to protect data being transmitted by employees working remotely. The NIST Data Security Framework would have reminded the company to consider network and endpoint security measures such as two-factor identification for remote employees, data encryption, and employee education about home network security.



Bruce is the equipment buyer for a multi-concept franchisee that operates more than 300 restaurants in a six-state area. While he typically works with only a few franchisor-approved equipment dealers, he's recently been purchasing replacement equipment from a local supplier for one of his company's chain concepts.

To expedite orders, the dealer suggests Bruce order what he needs online, but Bruce has had trouble getting the dealer's order entry process to mesh with his company's internal systems. The dealer recommends a third-party application programming interface (API) that's worked for other customers.

Bruce installs it on his mobile device, and it quickly links up his company's systems with the dealer's. Happy that the API worked as advertised, Bruce didn't give it a second thought.

Six months later, during an audit of the company's books, the company learns that someone has been stealing money from the company on a regular basis. After hiring a forensic accountant to find out how the money went missing, the company spends weeks and thousands of dollars to learn that a hacker had used vulnerabilities in the API to get into the company's cloud account. Once there, the hacker easily set up a way to siphon off funds from the company to a fraudulent account.

Had the company's IT department employed the NIST Framework, it would have recognized the importance of reviewing third-party APIs, requiring their use of multi-factor authentication (MFA) on all devices, and implementing more fail-safes such as data encryption and off-site data backup in addition to its cloud servers.



Terri manages operations for a multi-store restaurant group in a growing metropolitan area. 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.

Now she wonders if her hands-off approach makes her company vulnerable. While reading a story about hacked employee W-2 forms, 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.

Reviewing the company's data security plan that she'd put in place, she sees that 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. Remembering that the consultant she'd used had recommended the NIST Framework, she brought up data security at the next staff meeting and suggested using it to help organize all the different aspects of data security.

Now, the company enforces password protections and safeguards sensitive employee records and accounting systems. Terri also asked an outside security firm to check the company's computers to ensure no malware had been installed.





Sam is a successful, independent restaurateur. His restaurant has been getting good reviews and is growing fast—maybe a little too fast.

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

Sam survived the forensics audit but had to pay a substantial fine. The audit indicated that Sam's systems lacked adequate firewalls between secured and unsecured systems and networks; spam filters; and up-to-date antivirus and anti-malware software. In addition, it showed a vulnerability in the hand-off between his Wi-Fi network and certain 5G networks, putting customers' mobile payments at risk.

He hired a managed services provider to help him track his compliance with the Payment Card Industry Data Security Standard (<u>PCI DSS</u>). Sam and his team now use the NIST Data Security Framework to guide year-round data security planning.

Creating a Data Security System

Creating a data security program for your restaurant begins with reviewing the way you do business, assessing where you're vulnerable, reducing risks, and conscientiously making improvements on an ongoing basis. It's important to get into the right mindset as you start your planning. The **NIST Framework**, comprised of 5 core functions, is not a to-do list. It's a way of organizing your approach to data security and can be adapted and scaled to any operation. Before you begin your data security planning, the framework can help make sure you're covering key bases.



About the Data Security Framework

Pelcome to the nitty-gritty of "Digital Security 201." In this section, we provide a RESTAURANT-SPECIFIC version of the NIST Data Security Framework to help guide you in securing your restaurants' data. These steps apply whether you operate a small restaurant, a mid-size regional chain, or a large restaurant company. We recognize the process can feel daunting.

A FEW STARTING NOTES

• This is a process. You don't have to accomplish 100% 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 give you a starting point. Identify some critical items and start there.

• We're attempting 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.

• 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 this framework will be useful in keeping you on the right path.

HOW WE GOT HERE

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

To come up with this restaurant-specific digital security framework, our team:

- Reviewed the nearly 100 subcategories within the NIST Framework's 5 core functions.
- Inserted restaurant-specific action steps and
- outcomes for each subcategory.
- Rated each subcategory for its level of importance



ABOUT THE IMPORTANCE/ DIFFICULTY RATINGS

Level of importance/criticality

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 data. Here's how we 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 d	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 addressed.



Not sure where to start?

Within the NIST Framework's 5 core functions (Identify, Protect, Detect, Respond and Recover), the framework offers nearly 100 directives for companies to think about as they set up their data security protocols.

We include overviews of them all in the following pages and we've rated them by urgency (Criticality) and how hard they are to execute (Difficulty) based on input from our team of restaurant data security professionals.

As you plan, you may want to begin with the items the team rated as Urgent. We've collected them here for an upfront look—a starting guide to the most critical actions to consider when protecting data.

These 18 urgent items are a good start to your approach.

Disclaimer: 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 data security experts as you develop your plans.

••••• Urgent Action Items

C IDENTIFY

You've mapped out how your organizational communications and data flow. (Find it under ID.AM-3, p. 17)

Questions to ask

Has someone with IT experience diagrammed how information moves through 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 you complete this action

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 and describe the relative risk to the business.

You've established dependencies and critical functions for delivery of critical services. (Find it under ID.BE-4, p. 19)

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 and/or service providers required to deliver these services? Do you understand the consequences if these services aren't available? Do you have a backup plan?

Anticipated outcomes if you complete this action

You and your staff have thought through and understand what critical services are needed to run your business and the key functions you need to provide those services.



Q IDENTIFY (CONT.)

You understand and are managing legal and regulatory requirements regarding data security, including privacy and civil liberties obligations. (Find it under ID.GV-3, p. 20)

Questions to ask

Does the person (and/or your managed service provider) who oversees the IT function in your restaurant keep up with changing industry standards and regulatory requirements? Does that person/team provide you with updates? Do you review these updates with senior managers to determine if you need additional controls?

Anticipated outcomes if you complete this action

The organization should be mindful of the constantly changing legal environment and industry standards related to data security. 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.

Threats, both internal and external, are identified and documented. (Find it under ID.RA-3, p. 22)

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 Association's membership department to learn more about our resources.)

Anticipated outcomes if you complete this action

Develop a list of threats to your operation and update them. This covers all threats, including outside and within the organization, those of a technical nature and those of a human nature. You don't 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.

Risk management processes are established, managed and agreed to by organizational stakeholders. (Find it under ID.RM-1, p. 22)

Questions to ask

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

Anticipated outcomes if you complete this action

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



PROTECT

You are managing remote access. (Find it under PR.AC-3, p. 25)

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 they need to access? Do you keep a log of who's accessing your system?

Anticipated outcomes if you complete this action

Remote access includes internal business connections, service providers and third-party data connections. All 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.

You are managing access permissions and authorizations, incorporating the principles of "least privilege" and "separation of duties." (Find it under PR. AC-4, p. 25)

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 you complete this action

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.

You have protected network integrity and incorporated network segregation and segmentation where appropriate. (Find it under PR.AC-5, p. 25)

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 you complete this action

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; looks for potential risks) 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.



PROTECT (CONT.)

Identities are proofed and bound to credentials and asserted in interactions. (Find it under PR.AC-6, p. 25)

Questions to ask

Have you eliminated group accounts to better focus tracing and auditing? Have you implemented multi-factor authentication tools to prove identities?

Anticipated outcomes if you complete this action

Data and actions in systems are trackable and assured.

Your physical facility and cybersecurity personnel understand their roles and responsibilities. (Find it under PR.AT-5, p. 27)

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 you complete this action

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 go through an appropriate level of training and review. Any mistake at this level can be critical.

You protected communication and control networks. (Find it under PR.PT-4, p. 37)

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 you complete this action

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

You are monitoring to detect potential data security events. (Find it under DE.CM-1, p. 39)

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 no longer associated with a business process? Do you encrypt sensitive stored information and require a secondary authentication mechanism to access it?



((•))) DETECT (CONT.)

Anticipated outcomes if you complete this action

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.

You are detecting malicious code. (Find it under DE.CM-4, p. 40)

Questions to ask

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

Anticipated outcomes if you complete this action

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.



You execute the response plan during or after an incident. (Find it under RS.RP-1, p. 42)

Questions to ask

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

Anticipated outcomes if you complete this action

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.

You share information consistent with response plans. (Find it under RS.CO-3, p. 42)

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 you complete this action

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



RESPOND (CONT.)

You coordinate with stakeholders consistent with response plans. (Find it under RS.CO-4, p. 42)

Questions to ask

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

Anticipated outcomes if you complete this action

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

You understand the impact of the incident (Find it under RS.AN-2, p. 43)

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 you complete this action

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



You are managing public relations. (Find it under RC.CO-1, p. 45)

Questions to ask

Are you managing the public relations fallout from the incident?

Anticipated outcomes if you complete this action

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



The Framework for Restaurants

Our cybersecurity framework for the restaurant industry parallels the National Institute of Standards and Technology's Cybersecurity Framework. For each of the NIST Framework's 5 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.

Our team of restaurant cybersecurity experts then 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
٩,	IDENTIFY	Asset Management (ID.AM) Business Environment (ID.BE) Governance (ID.GV) Risk Assessment (ID.RA) Risk Management Strategies (ID.RM)	
A	PROTECT	Supply Chain Risk Management (ID.SC) Access Control (PR.AC)	23
		Awareness and Training (PR.AT) Data Security (PR.DS) Information Protection Processes and Procedures (PR.IP) Maintenance (PR.MA) Protective Technology (PR.PT)	
(((•)))	DETECT	Anomalies and Events (DE.AE) Security Continuous Monitoring (DE.CM) Detection Processes (DE.DP)	
• • •	RESPOND	Response Planning (RS.RP) Communications (RS.CO) Analysis (RS.AN) Mitigation (RS.MI) Improvements (RS.IM)	42 42 43 43 43 44
0	RECOVER	Recovery Planning (RC.RP) Improvements (RC.IM) Communications (RC.CO)	



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 organizational 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:

- 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.
- 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

owner

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.
- Include any other required licenses such as client access licenses (CALs) or related system requirements for use.

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.
- Update and revise your documents as changes are made and/or on a periodic basis.
- 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:

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

business use, purchase date and business

include type, name, version, license number,

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.AM-4

External information systems are catalogued

How to apply in your restaurant:

- Document all external systems, and code the systems for tracking, including type of system, data risk and locations.
- Update documentation of all external systems whenever there are changes to those systems.
- 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 containing sensitive and critical data and/or supports critical business objectives.







ID.AM-5

Resources (e.g., hardware, devices, data, time, personnel and software) are prioritized based on their classification, criticality, and business value

How to apply in your restaurant:

- 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 to achieving the business objective and value provided to the business. The priority can provide guidance to securing and upgrading your technology.



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:

- 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 (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.



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:

- 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.
- 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.





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:

- 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.



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

How to apply in your restaurant:

- 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

ID.BE-4

Dependencies and critical functions for delivery of critical services are established

How to apply in your restaurant:

- Create a list of services that are critical to running your business.
- Document and communicate any technology, vendor relationships or service providers that are required to deliver those services.
- 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.



ID.BE-5 Resilience requirements to support delivery of critical services are for all operating states (e.g., under duress/attack, during recovery, normal operations)

How to apply in your restaurant:

- 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.
- 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.







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 cybersecurity policy is established and communicated

How to apply in your restaurant:

- 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.
- An appropriate level of leadership (i.e., CIO, GC, CEO, etc.) should review and approve all information security policies.
- Communicate the policy to all appropriate company employees (annually is recommended).
- 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.



Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners

How to apply in your restaurant:

ID.GV-2

- 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.



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:

- IT subject matter experts should be well informed of ever-changing industry standards and regulatory requirements, and provide ongoing updates to the organization.
- IT subject matter experts should meet at least annually to discuss regulations and potential risks to the organization (see ID.RM-1).
- 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.





Governance (ID.GV) continued

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

How to apply in your restaurant:

- Meet with your board and/or management team at least annually to discuss risks to the company, including cybersecurity risks.
- 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.



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:

- Review the network diagrams to assess and document vulnerabilities (see ID.AM-3).
- 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.
- 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.



ID.RA-2 Cyber threat intelligence is received from information sharing forums and sources

How to apply in your restaurant:

- Review ID.AM-1 and ID.AM-2 to identify threatprotection 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.
- As part of your risk management strategy, evaluate options for automated updates and determine their suitability.
- 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.).



DIFFICULTY



Risk Assessment (ID.RA) continued

ID.RA-3 Threats, both internal and external, are identified and documented

How to apply in your restaurant:

- Determine sources of information about threats (industry resources like NRA, external sources identified in ID.RA-2, providers of threat-protection systems and internal subject matter experts).
- Establish a structure for gathering and documenting threat information that complements the needs of all steps in the risk assessment process.
- 3) Consolidate all threat information into this format.

Anticipated outcomes if action completed:

Develop a list of technology threats to your operation and update them on a regular basis. Consider 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; these will be addressed by other elements of the overall risk assessment strategy.)



DIFFICULTY

ID.RA-4 Potential business impacts and likelihoods are identified

How to apply in your restaurant:

- IT subject matter experts review the network diagrams to identify potential business impacts and likelihoods.
- Management (CIO, GC, CEO, etc.) reviews the assessment.

Anticipated outcomes if action completed:

Your organization reviews the impact and likelihood of a cybersecurity threat based on your unique business environment.

Anticipated outcomes if action completed:

Your organization ranks the business risk from low to high based on known cybersecurity

ID.RA-5 Threats, vulnerabilities, likelihoods, and impacts are used to determine risk

information.

How to apply in your restaurant:

- IT subject matter experts rank the identified business impacts and likelihoods based on the risk
- Management (CIO, GC, CEO, etc.) reviews the assessment.

ID.RA-6 Risk responses are identified and prioritized

How to apply in your restaurant:

- IT subject matter experts identify the risk responses and prioritize them based on their impact on the business.
- Management (CIO, GC, CEO, etc.) reviews the assessment.

Anticipated outcomes if action completed: Based on the risk ranking, your organization identifies and prioritizes the responses.



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

How to apply in your restaurant:

- 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? certain priorities?).
- 3) For those risks that are reviewed, document the response and rationale and then share with all relevant parts of the organization.

Anticipated outcomes if action completed: Establish a risk-assessment process with regular reviews by key members of your organization.





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.
- Review the risk tolerance represented by the approved mitigation activities to ensure consistency and appropriateness.
- 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.



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:

 As part of your overall risk-management strategy, regularly consult with peers in other organizations (if possible) and industry resources (e.g., NRA) 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.



NIST CATEGORY: Supply Chain Risk Management (ID.SC)

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.

ID.SC-1 Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders

How to apply in your restaurant:

- Question your vendors during contract negotiations about their internal security, including software update security.
- 2). Read "release notes" accompanying any updates and only apply releases once you're assured the updates have been reviewed for possible threats.
- 3) If you need to follow a strong "change management" procedure to roll out new information, and the update release is not critical, delay the release to get consensus from others that the updates are safe.

Anticipated outcomes if action completed:

The vendor partners that support your critical and network systems know they are held to a high security standard. You will be protecting your systems from supply chain cyberattack.



ID.SC-2 Suppliers and third-party partners of information systems, components and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process

How to apply in your restaurant:

- 1) List all vendors that deliver updates to critical systems and network.
- 2). Rank each one for impact of risk of system loss and potential for broad cyber infiltration.

Anticipated outcomes if action completed:

You'll have identified the vendors whose systems, if compromised, pose the most risk to your operation. You know to give them the most attention when managing their software updates.





Anticipated outcomes if action completed:

The vendor partners you select will pose less of

a risk for cyberattacks through the supply chain.



Supply Chain Risk Management (ID.SC) continued

ID.SC-3 Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's data security program and Cyber Supply Risk Management Plan

How to apply in your restaurant:

- During your vendor contracts review, review the companies' security standards and certifications.
- Ask for standards on testing and secured updates in this review.

ID.SC-4 Suppliers and third-party partners are routinely assessed using audits, test results or other forms of evaluations to confirm they are meeting their contractual obligations

How to apply in your restaurant:

 In contracts, ask vendors to maintain security and certifications and to be ready to provide new security attestations upon request. Anticipated outcomes if action completed: You'll work with vendor partners who have good security controls and who can prove they stay in compliance.



CRITICALITY

DIFFICULTY

Response and recovery planning and testing are conducted with suppliers and third-party providers

How to apply in your restaurant:

ID.SC-5

- Review "backout" or "roll back" procedures for all critical systems to ensure you can undo an update.
- 2) Discuss these procedures with vendor partners. Ask for clear backout procedures.

Anticipated outcomes if action completed:

There's an alternative plan to recover from an update-based supply chain attack beside waiting for a new update from the vendor.



NIST CATEGORY: Identity Management, Authentication and Access Control (PR.AC)

Access to physical and logical assets and associated facilities is limited to authorized users, processes and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions

PR.AC-1 Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes

How to apply in your restaurant:

- 1) Require unique accounts for each individual who accesses a POS terminal.
- Require unique credentials for each user who logs on to network devices.
- 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.



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.
- 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.







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 PCI cardholder data network should require two-factor authentication.



PR.AC-4 Access permissions and authorizations 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.



Network integrity is protected (e.g., network segregation, network segmentation)

How to apply in your restaurant:

PR.AC-5

- 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 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.AC-6

Identities are proofed and bound to credentials and asserted in interactions

How to apply in your restaurant:

- 1) Eliminate group accounts so you can trace sources and audit more efficiently.
- Use multi-factor authentication tools to verify 2) identities.

Anticipated outcomes if action completed:

Data and actions in systems are trackable and assured.





Access Control (PR.AC) continued

PR.AC-7

Users, devices and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks, and other organizational risks).

How to apply in your restaurant:

- Ask all vendor partners accessing your systems to use multi-factor authentication.
- 2) Use remote access software that uses multi-factor authentication.
- 3) Require all team members with access to secure data to use multi-factor authentication.

Anticipated outcomes if action completed: Your system will no longer be as vulnerable to password re-use and phishing attacks, increasing overall security.



NIST CATEGORY: Awareness and Training (PR.AT)

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

How to app	y in your restaurant:	Anticipated outcomes if action completed:	CRITICALITY
 Dissemi Perform approve Provide (based of 	nate security policies to all applicable users. annual reviews of all policies, and provide d versions to all applicable users. security-related training to all applicable users in position) on a regular basis.	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.	
 Train ne related 	w users (based on position) on security- policies upon hire.		
5) Acquire	sign-off from all users at least annually.		

How to apply in your restaurant:

- 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 their roles and responsibilities

How to apply in your restaurant:

- 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.





Awareness and Training (PR.AT) continued

PR.AT-4 Senior executives understand their roles and 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.

PR.AT-5 Physical and cybersecurity personnel understand their roles and responsibilities

How to apply in your restaurant:

- 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.
- Include specific line responsibilities for security personnel to ensure guidelines are set for granting permissions to other users.
- Review and require sign-off of all policies on a regular basis for security personnel.
- 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: 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.



Anticipated outcomes if action completed:

Security personnel provide a unique challenge to any security program. They have the right to change both user permissions and security settings/configurations. Due to this advanced ability, it is imperative that these personnel are properly selected and provided an appropriate level of training and review. Any mistake at this level can be critical.



1 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:

- 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 personal 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.





Data Security (PR.DS) continued

PR.DS-2

Data-in-transit is protected

How to apply in your restaurant:

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

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.



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

How to apply in your restaurant:

- 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.



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 throughout an organization.



Data Security (PR.DS) continued

PR.DS-5 Protection against data leaks are implemented

How to apply in your restaurant:

- 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.
- 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.
- 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.



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

How to apply in your restaurant:

- 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.
- 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



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:

- Separate development/test environments from production environments and put access controls in place to enforce separation.
- Segregate duties between personnel assigned to the development/test environments and those assigned to the production environments.
- Do not use production data (credit card, customer/ employee PII) for testing or development.
- Remove test data accounts from production before going live.
- Change control procedures related to security patches, and document software modifications.

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.



PR.DS-8 Integrity-checking mechanisms are used to verify hardware integrity.

How to apply in your restaurant:

- 1) Require your vendor to use tamper-proof or tamper-evident hardware
- 2) Inspect hardware for signs of tampering on a regular basis such as credit-card devices.

Anticipated outcomes if action completed:

You maintain the integrity of the hardware used in the restaurant.







1 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 incorporating security principles (e.g., concept of least functionality)

How to apply in your restaurant:

- 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.





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:

- 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.
- 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 systems 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

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

How to apply in your restaurant:

- 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 net 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.



PR.IP-4

Backups for information are conducted, maintained, and tested

How to apply in your restaurant:

- 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.
- 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.







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:

- 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.
- Include a review of the physical data center environment in your contracts and relationships with third-party service providers.

PR.IP-6 Data is detroyed according to policy

How to apply in your restaurant:

- During a POS or back-office-system refresh, sanitize (destroy) end-of-life hard drives prior to the equipment leaving your restaurant's possession.
- 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:

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.



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.









DIFFICULTY

Information Protection Processes and Procedures (PR.IP) continued

PR.IP-7 Protection processes are improved

How to apply in your restaurant:

- 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.
- 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.

PR.IP-8 Effectiveness of protection technologies is shared

How to apply in your restaurant:

- 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.
- 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

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:

- 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.
- 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

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

DIFFICULTY

34





Information Protection Processes and Procedures (PR.IP) continued

PR.IP-10 Response and recovery plans are tested

How to apply in your restaurant:

- 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.



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

How to apply in your restaurant:

- 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).



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

How to apply in your restaurant:

- Conduct vulnerability scans (internal and external systems) monthly to identify and classify known vulnerabilities.
- Apply a repeatable approach to remediating identified vulnerabilities based on the severity and projected impact on your business.
- 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.







1 NIST CATEGORY: Maintenance (PR.MA)

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

PR.MA-1 Maintenance and repair of organizational assets are performed and logged with approved and controlled tools

How to apply in your restaurant:

- Vet your IT equipment service providers to confirm that they have the required skills, toolsets, regulatory requirements and certifications to support your IT assets.
- Remove from service any IT equipment that is not performing correctly until repairs can be completed.
- 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.



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:

- 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.



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.
- Centralize the collection of security event log data from all devices.
- 4) Retain security event logs in accordance with policy. Chec with PCI for the latest requirements for the PCI Data Security Standard.
- 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.





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:

- 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.
- 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.



PR.PT-3 The principle of least functionality is incorporated by configuring systems to provide only essential capabilities

How to apply in your restaurant:

- 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.
- Log all access to systems, including invalid login attempts.
- Require unique accounts for each user and log access to network devices, appliances and other managed devices.
- 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.



PR.PT-4 Communications and control networks are protected

How to apply in your restaurant:

- Limit access to network technologies such as MPLS, DSL and cable connections to authorized users and networks.
- Limit access to networks used for the management of systems such as DRAC, SNMP and SSH 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.

PR.PT-5

Mechanisms, e.g., fail-safe, load balancing, hot swap, are implemented to achieve resilience requirements in normal and adverse situations. (Fail safe: a way to terminate system functions to prevent damage; load-balancing: distributing the amount of work between several computers so that lots of work can be performed at the same time; hot swap: replacing hard drive, power supply, other device while the computer using it is still operating.)

How to apply in your restaurant:

 All critical systems need these kinds of business continuity plans to assure uptime with least impact when a cyber event occurs.

Anticipated outcomes if action completed:

Systems have plans/means to keep operating in the event of a cyberattack.







NIST CATEGORY: Anomalies and Events (DE.AE)

Anomalous activity is detected 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:

- Establish baseline configurations for information systems and system components, including communications and connectivity-related aspects of systems.
- 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.



DE.AE-2 Detected e

Detected events are analyzed to understand attack targets and methods

How to apply in your restaurant:

- 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:

Anticipated outcomes if action completed:

an easily accessible area in case they are

Anticipated outcomes if action completed:

tion systems and implement alternative

Develop contingency plans to restore informa-

mission/business processes when systems are

needed for investigations.

compromised.

Store audit records for security-related events in

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



CRITICALITY

DIFFICULTY

CRITICALITY

DIFFICULTY

CRITICALITY

DIFFICULTY

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

How to apply in your restaurant:

 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.

DE.AE-4 Impact of events is determined

How to apply in your restaurant:

- 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.

DE.AE-5 Incident alert thresholds are established

How to apply in your restaurant:

- 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.
- 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.



NIST CATEGORY: Security Continuous Monitoring (DE.CM)

The information system and assets are monitored 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:

- 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.



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

How to apply in your restaurant:

- Develop a continuous monitoring strategy and implement a continuous monitoring program.
- 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).



DE.CM-3

3 Personnel activity is monitored to detect potential cybersecurity events

How to apply in your restaurant:

- Record user activities, exceptions, faults and information security events in a log, and regularly review the logs.
- 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.



Respond



Security Continuous Monitoring (DE.CM) continued

•		
DE.CM-4 Malicious code is detected		
<i>How to apply in your restaurant:</i> Use malware detection 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 worksta- tions and endpoints infected by the attack. Determine infiltration methods and consider adjustments to defenses.	CRITICALI
DE.CM-5 Unauthorized mobile code is detec	ted	
<i>How to apply in your restaurant:</i> Use malware detection tools to detect unauthorized code on mobile devices, and alert security personnel.	Anticipated outcomes if action completed: 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.	CRITICALI DIFFICULT
DE.CM-6 External service provider activity is m	onitored to detect potential cybersecurity o	events
<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.	Anticipated outcomes if action completed: 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.	CRITICALI
DE.CM-7 Monitoring for unauthorized person is performed	nnel, connections, devices, and software	
<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.	<i>Anticipated outcomes if action completed:</i> The security incident is contained and the information is available for a security review (forensics).	
DE.CM-8 Vulnerability scans are performed		
How to apply in your restaurant:	Anticipated outcomes if action completed:	CRITICALI

Perform scans to detect medium-to-low risk and high-risk vulnerabilities to the system.

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.







NIST CATEGORY: Detection Processes (DE.DP)

Detection processes and procedures are maintained and tested to ensure 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.
- 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.



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

How to apply in your restaurant:

- 1) Develop and implement a detection process.
- 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.
- 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.



DE.DP-3 D

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 a blocked. If this is not the case, remedy the situation and test again.



DE.DP-4

4 Event detection information is communicated

Detection processes are continuously improved

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.



DE.DP-5

- How to apply in your restaurant:
- 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.





NIST CATEGORY: Response Planning (RS.RP)

Response processes and procedures are executed and maintained to ensure response to detected cybersecurity incidents.

RS.RP-1

P-1 Response plan is executed during or after an incident

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:

Your event will be shorter in duration, 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 if you have a plan.



NIST CATEGORY: Communications (RS.CO)

Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies).

How to apply in your restaurant:	Anticipated outcomes if action completed:	CR
Notify your security team and managers when an event occurs. Ensure that your team knows their roles and how to respond.	During a security event, all personnel will know their roles, and the response plan will be implemented quickly.	DII
RS.CO-2 Incidents are reported consistent	with established plan	
How to apply in your restaurant:	Anticipated outcomes if action completed:	CR
Have a plan in place that spells out what needs to be	The correct people in and outside your organiza-	
communicated to whom when an event occurs.	tion are informed.	DI
RS.CO-3 Information is shared consistent w	vith response plans	
How to apply in your restaurant:	Anticipated outcomes if action completed:	CF
Develop a crisis communications plan, and follow it during	Inform the appropriate stakeholders (vendors,	•
respond.	needed for recovery with your partners.	DI
RS.CO-4 Coordination with stakeholders of	ccurs consistent with response plan	
How to apply in your restaurant:	Anticipated outcomes if action completed:	C
Consistently update your stakeholders so they can help	Relevant members of your team will be working	•
reduce the impact of an incident.	restaurant functional. Information, including sensitive legal information, will be restricted to	DI

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.







NIST CATEGORY: Analysis (RS.AN)

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

RS.AN-1 Notifications from detection systems are investigated How to apply in your restaurant: CRITICALITY Anticipated outcomes if action completed: Review alerts immediately with your personnel/vendors Your team should respond to any unusual alerts. from any systems that send alerts, such as virus and and Investing in tools or partnerships that enhance DIFFICULTY your monitoring capabilities will make this task network-security tools. less difficult. RS.AN-2 The impact of the incident is understood Anticipated outcomes if action completed: CRITICALITY How to apply in your restaurant: Understand that as an event begins, your first discoveries Determine the extent of the problem so you can may not be the source of the problem. As an example, one fully resolve it. DIFFICULTY 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. RS.AN-3 **Forensics are performed** How to apply in your restaurant: Anticipated outcomes if action completed: CRITICALITY In the event of a major breach of your systems, perform a You will understand fully what happened in the forensics audit. Consult immediately with a forensics incident and know when it is resolved. DIFFICULTY expert to ensure that you are properly maintaining evidence and can mitigate the breach as soon as possible. RS.AN-4 Incidents are categorized consistent with response plans How to apply in your restaurant: Anticipated outcomes if action completed: CRITICALITY Follow your response plan to ensure clear thinking and Following your response plan ensures that you that appropriate actions are taken. correctly respond to an event. DIFFICULTY RS.AN-5 Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers) CRITICALITY How to apply in your restaurant: Anticipated outcomes if action completed: 1) Read all security bulletins from partners and reliable You reduce the chance of being broadsided by a security sources. threat because you are aware of them and DIFFICULTY 2) Scan your systems for vulnerabilities using tools. preemptively managed for them.

NIST CATEGORY: Mitigation (RS.MI)

Activities are performed to prevent expansion of an event, mitigate its effects, and resolve 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).







Mitigation (RS.MI) continued

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.



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.



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					
<i>How to apply</i> Having a mee learned.	<i>in your restaurant:</i> ting after every incident to discuss lessons		Anticipated outcomes if action completed: An evolving plan that improves with time will reduce the likelihood and impact of a similar event.		CRITICALITY
 RS.IM-2	Response strategies are updated	l			
How to apply	<i>in your restaurant:</i> to respond starts with a plan rather than the		Anticipated outcomes if action completed:		

experience itself. Always update your plans.

gained from each response to an incident.



NIST CATEGORY: Recovery Planning (RC.RP)

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

Recovery plan is executed during or after a cybersecurity incident

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.





document that grows with your business and

adapts to new threats. Apply the lessons you

have learned so you don't repeat past mistakes.



DIFFICULTY

NIST CATEGORY: Improvements (RC.IM)

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

Recovery plans incorporate lessons learned CRITICALITY How to apply in your restaurant: Anticipated outcomes if action completed: Your recovery plan should incorporate lessons learned Your response plan evolves and becomes from responding to the incident. For example, if an stronger over time. DIFFICULTY 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. **Recovery strategies are updated** How to apply in your restaurant: Anticipated outcomes if action completed: CRITICALITY Learn from real security incidents, and use those lessons Recognize that your response plan is an evolving

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.

NIST CATEGORY: Communications (RC.CO)

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

RC.CO-1 Public relations are managed		
<i>How to apply in your restaurant:</i> Implement a crisis communications plan to manage the public relations fallout from the incident. Consider hiring an outside PR consultant to help you.	<i>Anticipated outcomes if action completed:</i> Customers fully understand that you are doing everything you can to mitigate the event.	CRITICALITY
RC.CO-2 Reputation is repaired after an inc	ident	
<i>How to apply in your restaurant:</i>	<i>Anticipated outcomes if action completed:</i> A fully informed customer will remain a custom-	

Recovery activities are communicated to internal and external stakeholders as well as executive and management teams

How to apply in your restaurant:

PR partners when available.

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.

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

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.





Keeping Payment Data Safe

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 an overview in the 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?

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% guarantees that you won't experience a data 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	 Install and maintain a firewall configuration to protect cardholder data Do not use vendor-supplied defaults for system passwords and other security parameters 		
Protect cardholder data	 Protect stored cardholder data Encrypt transmition of cardholder data across open, public networks 		
Maintain a vulnerability management program	 Use and regularly update anti-virus software or programs Develop and maintain secure systems and applications 		
Implement strong access control measures	 Restrict access to cardholder data by business need-to-know Assign a unique ID to each person with computer access Restrict physical access to cardholder data 		
Regularly monitor and test networks	 Track and monitor all access to network resources and cardholder data Regularly test security systems and processes 		
Maintain an information security policy	12. Maintain a policy that addresses information security for employees and contractors		





Digital Security 201

Sponsored by

