Food Ag ISAC

An IT ISAC Community

Cybersecurity Guide for Small and Medium-Sized Businesses

2025

TABLE OF CONTENTS

INTRODUCTION

The food and agriculture sector, like all critical infrastructure sectors, faces a complex range of cybersecurity threats. Like any modern business, organizations in the industry rely on technology for essential operations and administration. However, it also uniquely integrates technology into areas like food processing, agricultural machinery, precision farming, and the storage and transportation of goods.

Given the interconnectedness of the food and agriculture ecosystem, every business, regardless of size, must prioritize securing its digital assets. While cybersecurity is often perceived as a concern primarily for large corporations, small and medium-sized businesses (SMBs) are often more vulnerable due to limited resources and cybersecurity expertise. Protecting small and medium-sized businesses ensures a secure and resilient sector.

In 2023, the first edition of the Food and Ag Cybersecurity Guide for Small and Medium-Sized Enterprises was released, offering practical and affordable security practices that SMBs in the sector can implement to enhance their resilience and cyber posture. The guide was an integral step in assisting SMBs in bolstering their defenses. In late 2024, the Food and Ag-ISAC released the first-ever **Food and Ag Sector Cyber Threat Report** that focused specifically on cyber threats to the food and agriculture industry. The report highlighted metrics on over 50 adversaries active within the sector, finding the following list of common TTPs and the percentage of these adversaries who leveraged them. Even though a technique was used less commonly, it does not make it less relevant. This list provides a baseline for common adversary techniques and may help organizations prioritize their efforts.

- Living-off-the-Land (LOTL) (92%)
- Phishing and Spear Phishing (88%)
- Custom Malware and Tools (80%)
- Stealthy Exfiltration Techniques (70%)
- Lengthy Persistence and Defense Evasion (70%)
- Data Encrypted for Impact (66%)
- Zero-Day Vulnerabilities (43%)
- Modifying Existing Malware and Tools (35%)
- Destructive Techniques (25%)
- Supply Chain Compromise (23%)
- Disruptive Attacks (21%)

This year, we have refreshed the Food and Ag Cybersecurity Guide for Small and Medium-Sized Enterprises to reflect the findings of the Food and Ag Cyber Threat Report. This new guide includes updates to previous security practices and new steps enterprises can take to enhance cyber protection. While no company or network is entirely immune to cyber threats or attacks, the following practices offer effective ways to manage risks from threats currently affecting the industry. Many of these practices can be implemented at no or relatively low cost – minor, inexpensive changes in an organization's cybersecurity efforts can often make a significant difference in preventing incidents from occurring.

Implementing these security practices (or some of them) can reduce the likelihood that your company will become a victim of a successful attack and strengthen your organization's ability to recover if one occurs. These steps will not guarantee immunity from cyber attacks, but they will significantly reduce the likelihood of a breach and improve the organization's ability to respond effectively if an incident occurs.

SECURITY PRACTICE #1 Educate Before it’s Too Late

Security awareness training can help employees stop incidents before they occur.

Enacting and maintaining a strong cybersecurity posture for your organization begins with your employees: your first line of defense against potential attacks. Ensuring they have the knowledge and tools to identify and respond to suspicious activities is essential. An **estimated 68% of security breaches** across organizations involve a human element; however, these errors can be cut down upon with the proper training.

Implementing security awareness training provides key cybersecurity education across your organization and reduces the chances of a breach dramatically – **as much as 30%**. Though these programs may differ in content from organization to organization, they typically cover a wide range of topics, including password security, data privacy, and phishing awareness, which we will cover in more detail below. When your employees better understand the threat, they are more likely to implement sound security practices, follow security policies, and help recognize and prevent attacks. Employee training includes regular checks, tests, and re-training as time passes to keep knowledge and skills current.

Though the importance of security awareness training is not unique to the food and agriculture sector, companies in this sector are particularly likely to be targeted by social engineering attacks **such as phishing**. Implementing employee training is one of the easiest and most effective ways to majorly boost your organization’s cybersecurity.

SECURITY PRACTICE #2 No Phish Here

Be aware of phishing scams, how to spot them, and what to do if they occur.

Despite technological advances that have made cyber attacks more sophisticated over the years, low-tech phishing remains the most common way that cybercriminals get their foot in the door and steal information from organizations. Over **90% of successful cyber attacks** begin with phishing – and in the food and agriculture sector, this tactic is the **second most prevalent**. Odds are, you will end up with a malicious email in your inbox at some point. Attackers often send emails with alarming headlines or impersonate recognizable company names. The goal is to get the victim to click on a link or file, which will then download malicious software onto their device.

Sometimes these emails come from our most trusted colleagues (or so it seems) – business email compromise (BEC) is a common form of attack where attackers impersonate trusted parties, or may even have compromised a known contact. Trust your gut: if anything seems off or suspicious, call (do not email) the person to confirm they contacted you before sharing any sensitive information.

Remember these important tips to avoid being on the hook for phishing (and check out our **phishing-specific blog here**):

- Do not open emails or download software from untrusted sources.
- Do not click on links or attachments in emails from unknown senders.
- Do not supply passwords, personal, or financial information via email to anyone (sensitive information is also used for double extortion).
- Always verify the email sender's email address, name, and domain.
- Protect devices using antivirus, anti-spam, and anti-spyware software.
- Report phishing emails to the appropriate security or IT staff immediately.

SECURITY PRACTICE #3 Patch It Up

Regularly patch your software to avoid vulnerabilities.

Food and agriculture organizations employ a wide variety of technology, including a range of software applications, to assist at every stage of the farm-to-table pipeline. However, when it comes to applications, vulnerabilities happen – and these vulnerabilities occur **just as commonly in manufacturing equipment** as they do in IT equipment. Even the most secure software can push updates that unintentionally introduce bugs and exploits, which cyber criminals may then leverage to get access to your information.

Applying patch updates is important, and regularly updating your team's tech ensures that software, firmware, and drivers are all as reinforced as possible against potential attacks. Stay in tune with your vendors, and always patch as soon as possible when updates are pushed through. When possible, enable automatic updates so that your devices receive updates as soon as the vendor releases them. In some cases, a patch may not be immediately available. In these instances, organizations should monitor the vendor's guidance for temporary mitigations or unplug systems until a patch is available.

SECURITY PRACTICE #4 MFA is the Way to Play

Always enable multi-factor authentication (MFA) for maximum account security.

Your password is your key to the kingdom, often providing open access to highly sensitive information – and yet **62% of people store their passwords in unsecured places**, such as on sticky notes left next to their computers. Passwords should be complex and stored in a secure location, such as a password manager. Many organizations are moving toward pass phrases. However, while passwords are important, they are no longer enough. Organizations should also enable **multi-factor authentication (MFA)** for any accounts that will allow them to do so.

MFA provides added protection if someone acquires (or guesses) an account's password. It requires a combination of two or more credentials to access your account and works by requesting something you have (phone) with something you know (password). This serves as an extra layer of protection. Even if an attacker obtained a password, they would also need access to a user's mobile device or mobile token to gain access to the account. Text message-based MFA is good, but application-based MFA is even better.

Many cybercriminals are opportunistic, targeting the easiest and most lucrative opportunities. The more difficult it is for an attacker to breach your information, the more likely they are to give up – keeping your accounts safer in the process. MFA is an easy and exceedingly cost-effective way for food and agriculture businesses to increase defenses against attackers.

SECURITY PRACTICE #5 Beware of Remote Monitoring and Management (RMM)

Recognize the dangers of RMM and proceed accordingly.

Remote monitoring and management, or RMM, refers to technology used to manage an organization's IT infrastructure remotely. Administrators use this technology to monitor settings and configure resources from a distance that may be stored in a data center or elsewhere. Many small and medium-sized businesses, including those in the food and agriculture sector make use of RMM to better oversee their technology – including computers, mobile devices, and servers – from a single access point.

However, as much as this technology helps, it also comes with its own set of risks. Adversaries commonly abuse RMM tools to get direct access to victim machines before moving laterally through the network. **Threat actors such as LockBit** have historically exploited these tools to enter and wreak havoc on victims' environments. In 2022, CISA **released an advisory** alerting organizations to be wary of the malicious ways that RMM can be used in attacks.

While some organizations rely on RMM for various reasons, knowing that attackers can breach these tools and knowing how to defend against their misuse is key. Enact these effective best practices to keep your organization safe:

- Enable MFA for all RMM programs you may be using, and maintain strong password security.
- Implement access control lists, audit access controls regularly, and ensure employees use a VPN during travel.
- Apply software patches immediately to prevent vulnerabilities.

SECURITY PRACTICE #6 Is That Allow(list)ed?

Apply a zero trust outlook on your organization.

The fewer applications that can make their way onto your employees' devices, the smaller the chance that something malicious can make its way there. Application allowlisting helps your IT team keep a tight handle on what can and can't be downloaded and used on company devices. Rather than setting up a blocklist for certain applications, allowlisting takes the opposite approach: all applications are blocked except for those that admins have permitted. This can stop malicious applications like malware from being downloaded and installed, even if an employee accidentally attempts to do so.

Application allowlisting aligns with the zero trust principle, which is an approach to security that defaults to distrusting requests and requires verification at all stages. Though allowlisting is an effective way to keep out unwanted and dangerous applications, only about a third of organizations have implemented it as of **2021, according to an IDG study**. Implementing application allowlisting is an effective way of blocking malicious activity.

SECURITY PRACTICE #7

Backup, Restore, and Recover - Trust and Test the Process

Ensure backups are stored offline and regularly test recovery procedures.

It's not a question of if a cyber attack or system failure will occur, but when. The speed at which you can recover and restore operations will often depend on how well your data is backed up, where those backups are stored, and your ability to recover them quickly.

Creating copies of critical data, systems, and files is essential for recovery. Backups can be stored in various ways, including on servers, in the cloud, and on physical drives. However, it is strongly recommended that all backup strategies include offline storage. Offline backups are disconnected from the internet, making them virtually immune to hacking, corruption, and ransomware encryption. Backups are a crucial line of defense for safeguarding your organization's most critical information.

In the food and agriculture sector, time-sensitive operations mean that any extended downtime can result in significant losses, including product spoilage, delivery disruptions, and regulatory non-compliance. Regular, secure, and tested backups are critical for restoring operations quickly and minimizing these risks. In 2024, backup adoption among small and medium-sized businesses (SMBs) **grew by 24% and 60% of companies** now back up data daily.

When working on backups, make sure to keep the following in mind:

✓ **Decide what to back up.**
Determine what is most critical to your business and prioritize backing up that data before moving to less important items. Organizations can have lots of data, and storage can become expensive – backing up only essential data can help organizations manage the lift.

✓ **Choose your backup method.**
Many backup solutions are available, regardless of whether you backup data on-premise or to a cloud solution. The most critical data should include an offline version to prevent adversary tampering.

✓ **Determine your backup location(s).**
Both on-premise backups and cloud solutions can be effective. On-premise solutions can offer more control, customization, and recovery times, but may require more maintenance. Cloud solutions are scalable, often more affordable, and maintained by a third party.

✓ **Set a regular backup schedule.**
Data should be backed up at regular intervals. Organizations will need to consider several metrics while determining this schedule. Mission-critical data that is updated frequently may require daily, hourly, or even continuous backups; important data that doesn't change as frequently may not need to be backed up as regularly.

✓ **Protect all backups.**
Ensure that whatever solution you choose has protections in place to ensure that adversaries cannot tamper with your backups. Having an offline version of your backups can be more resource intensive, but it is the only guaranteed way to ensure your backups are not impacted by a cyber incident.

✓ **Test your backups.**
It doesn't matter if you backup regularly and have several online and offline options for your information, if you don't know how to recover and restore. Practice makes perfect.

SECURITY PRACTICE #8 Seal the Deal by Encrypting Your Information

The critical role of data encryption in protecting sensitive information.

Adding another layer to your cybersecurity practices, like encryption, makes any accessed information unusable for attackers. Encrypting your data and files, whether at rest or in transit, helps to keep your sensitive information safe should an attacker gain access to your enterprise, or someone loses a laptop or storage drive. Imagine getting a treasure map, and the only way to find the “X” that marks the spot would be to have a specific magnifying glass or black light that can find the hidden information needed to complete your journey. Encrypted files or data require a proper decryption key to “open” or “decode” it.

Data encryption causes attackers to hit a wall in their efforts to collect critical and sensitive information. If the information hackers find is unusable, then it is valueless and thwarts the need to pay ransom or meet demands.

As members of the food and agriculture supply chain, organizations have a responsibility to protect their information – which may include partner and supplier details, logistics, and customer details.

SECURITY PRACTICE #9 Keep Watch Through Account Auditing and Monitoring

Leverage account auditing and continuous monitoring to support threat detection and early warning.

Account auditing and general monitoring are critical components of an organization’s cybersecurity posture, allowing for observation and analysis that can lead to the detection of anomalies, user access, and more.

Account auditing allows organizations to track access and logins, review inactive or abandoned accounts, detect policy violations, and observe patterns. Continually auditing can shine light on any unauthorized access, failed login attempts, large data transfers, and overall accountability for users. Items to consider checking during your account auditing include, but aren’t limited to: user access review, authentication logs, and account usage. **Over 75% of security leaders** view account takeovers as a major threat - never underestimate the power of watching and reviewing accounts.

With general monitoring, organizations can watch for user activity and traffic, observe cloud and endpoint operations, and track overall trends. Continual monitoring and quarterly auditing can help with early threat detection and incident response when the alarm sounds. Keep eyes out for large transfers of data; setting up alerts, if possible, can help to flag suspicious activity early.

In the food and agriculture industry, many supply chains and precision agriculture tech tools are connected to internal networks, making the exploitation of accounts or insider threats even more disruptive to operations. Finding these potential dormant or exploited accounts through account auditing or monitoring can help to stop impending malicious activity.

SECURITY PRACTICE #10 Don’t Fly Solo - Engage and Share with Your Peers

How threat intelligence sharing with peers and partners can help your cyber defense.

Talking openly to your employees, peers, and partners about cybersecurity is a key part of defending your enterprise. In 2025, 90% of organizations plan to invest more into their threat intelligence budgets, highlighting the importance of threat intel. Active threat intelligence sharing across all sectors, including the food and agriculture industry, strengthens collective defenses through calling attention to irregularities, potential vulnerabilities, and threats. Not only does sharing help organizations detect threats earlier it also helps them prepare and protect.

In cybersecurity, we all know that the faster a threat is detected, the faster it can be mitigated. No one organization has full visibility into the threat landscape, but by exchanging threat intel and insights, we can identify potential threats and how to respond to them faster. Sharing doesn’t need to be limited to only technical indicators, but also tactics, techniques, and procedures (TTPS), motivations, attributions, and any other relevant information. The more context, the more security teams can adjust their defenses appropriately.

Building collaboration and trust helps us all defend better, together no matter the industry. Talk to your peer companies so that you can learn from each other.

SECURITY PRACTICE #11 Keep Calm with an Incident Response Plan

Developing and regularly testing an incident response (IR) plan.

It is never too late to put an incident response (IR) plan in place. In any industry, disruption to systems can have cascading impacts that are not only costly but also impactful to reputation. A proactive and thorough IR plan should address how your organization can respond to and recover from a cybersecurity incident by outlining clear roles, responsibilities, procedures, and protocols. When you have to jump into action for a cyber threat, a comprehensive IR plan will eliminate any uncertainty or gaps regarding who to contact and what to do to restore normal operations quickly.

Documenting an incident response plan is only step one; testing the plan is the second step. Running exercises using your IR plan can help you address any issues or hurdles, as well as test the plan's effectiveness. At minimum, IR plans should be tested once a year, but more testing can equal more efficiencies.

SECURITY PRACTICE #12 Not Everyone Needs a Master Key or an All Access Pass

Implementing the principle of least privilege (PoLP) and role-based access control (RBAC).

The principle of least privilege (PoLP) and role-based access control (RBAC) are fundamental cybersecurity principles that help reduce risk and limit damage. Using PoLP or RBAC means giving users, systems, and applications the minimum level of access necessary to perform their job or role successfully. Through the implementation of PoLP or RBAC, you help to reduce insider threats (whether malicious or not), protect sensitive information, limit attack vectors, and help maintain system stability.

In the food and agriculture industry, seasonal and/or rotating staff are common, making consistent access control essential to prevent the misuse of systems, equipment, data, and other tools. It is equally important for other segments of the industry to limit and monitor access like cloud-based farm management platforms, smart irrigation systems, cold chain access controls, GPS, and more. Ensuring that the designated technicians or employees have access can help keep any threats or disruptions at bay.

To successfully implement least privilege practices, organizations need to identify all accounts, endpoints, and systems, as well as determine the access that is needed for each role or job. It is recommended to avoid blanket permissions and eliminate unnecessary admin access. Organizations should make sure to conduct access reviews two times a year at minimum. Another key step in PoLP and RBAC is offboarding employees and/or updating permissions should their role change. Based on a recent study, **34% of businesses have over 10 past employees** who can access their data. Employees leaving the company should be offboarded immediately to help eliminate risk or unauthorized access.

CONCLUSION

Building and maintaining a strong cybersecurity posture is essential for all organizations in the food and agriculture industry – no matter the size. For small and medium-sized businesses, protecting digital assets, operational systems, and sensitive data is vital to maintaining trust with key customers and partners and safeguarding the integrity of the supply chain.

As cyber threats continue to evolve, your defenses must as well. Implementing the above mitigations can help companies significantly reduce their risk of attack and improve their resilience without needing to invest an exorbitant amount of money or resources. On the contrary, these relatively small changes pay big dividends in protecting your information, leading to saved time and capital in the process.

Cyber defense is an ongoing process, but every effort helps to make your organization and the sector a safer place for all. We defend better when we defend together.

Food Ag ISAC

An IT ISAC Community

Launched in May 2023, the Food and Agriculture-Information Sharing and Analysis Center (Food and Ag-ISAC) provides threat intelligence, analysis, and effective security practices that help food and agriculture companies detect attacks, respond to incidents, and share indicators so they can better protect themselves and manage risks to their companies and the sector.

Visit us at **FoodAndAg-ISAC.org** or email us at **membership@foodandag-isac.org**.

Report published May 2025.