Food Ag-ISAC

Food and Agriculture Sector Cybersecurity Guide for Small and Medium-Sized Businesses

2026

TABLE OF CONTENTS

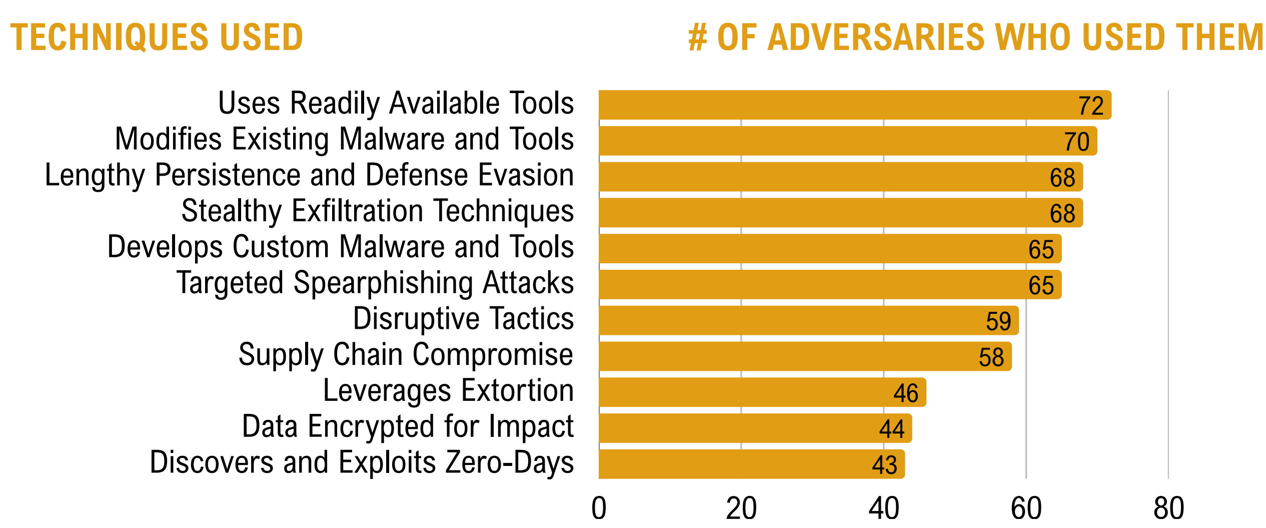
INTRODUCTION

In today's food and agriculture industry, technology helps us work faster and more efficiently, but it also changes the way we need to think about the security of our farms and ranches. According to our most recent 2025 Food and Agriculture Cyber Threat Report, the sector is increasingly being swept up in broad, automated cyberattacks. These aren't always personal or targeted; instead, hackers use "digital scanners" to find any open door, regardless of a business's size. For a small operation, the risk isn't just a computer glitch; it's the downtime that halts a harvest, disrupts a shipment, or freezes your accounts at the worst possible moment.

Small and medium-sized businesses (SMBs) often carry the greatest risk because they are the backbone of the industry. They might have fewer resources than a global corporation, but their role in keeping food on the table is just as vital. Securing the business isn't "extra" work - it is foundational to keeping your operation resilient.

In our most recent Cyber Threat Report, which focused on the food and agriculture sector, we analyzed the specific methods hackers use to target our industry. We tracked over 300 groups and narrowed down the 72 most active threats to see exactly how they get in. The good news? Most of them rely on the same handful of tricks.

Below are the different techniques used by more than half of the adversaries tracked for the sector.



This updated cybersecurity guide for SMBs builds on our original 2023 edition with new, actionable advice tailored specifically for food and agriculture companies. We know you have a business to run, so we've focused on cost-effective, easy-to-implement practices that manage the specific risks facing our industry today.

While no system is 100% immune, these steps will make your business a much harder target and ensure that if a problem does occur, you are prepared to get back to work quickly.

SECURITY PRACTICE #1 Access Control

Not Everyone is a VIP: Limit your master keys and all-access passes.

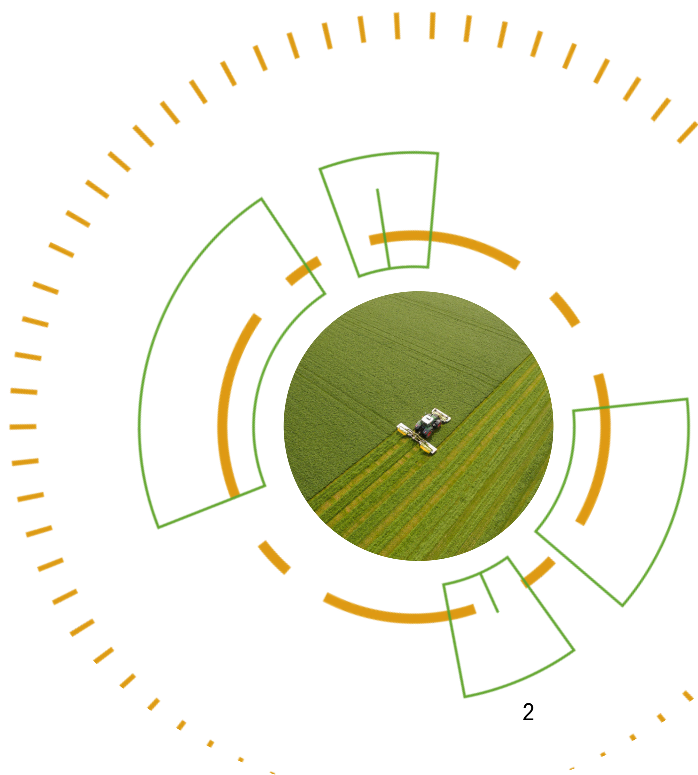
The most common way hackers operate today is by using readily available tools or by conducting “living-off-the-land” (LOTL) attacks. Instead of bringing their own specialized hacking software, they use the legitimate, "trusted" work tools already installed on your computers, like Windows PowerShell, remote desktop, or built-in scripting utilities. In the physical world, it is the difference between a burglar bringing their own crowbar versus finding the spare key you’ve hidden under a doormat.

For a small business, your best defense isn’t necessarily buying expensive new software but rather setting better house rules for your digital space, including who can do what and what programs are allowed to run.

- **Principle of Least Privilege** - *Controls who has access*
  Only give employees access to the specific files, systems, and permissions they need for their actual job. Most employees should use standard user accounts for daily work, while administrative accounts should be reserved for specific tasks and logged in when needed. For example, a driver doesn't need the administrative passwords for your accounting server. And if someone leaves, it is crucial to disable their access that day.

- **Application Allowlisting** - *Controls what programs can run*
  This is your organization's way of saying that a program is approved to run in that environment; if it isn’t, the system will shut it down. For example, there is no reason for someone in accounting to be running advanced scripting tools, and with allowlisting in place, this action would cease. It is important to remember that allowlisting is powerful and will require tuning - if you set it too strictly, employees can’t do their job while too passive and the benefit of it is lost.

If your organization runs on Windows, they already include built-in tools for no additional cost, AppLocker and Windows Defender Application Control (WDAC).



SECURITY PRACTICE #2 Backup, Restore, and Recover

Test the Process: Backups are only as good as the last time you tried to restore them.

Having a backup in place should an attacker take down or lock your system is the difference between reopening quickly or never reopening at all. For food and agriculture SMBs, it is important to remember that downtime can equate to spoiled product, halted harvests, missed shipments, and more. Luckily, effective backup practices don't require enterprise budgets, but it is important to ensure they're in place and usable.

✓ **Follow the 3-2-1 rule.**
Keep three copies of your critical data on two different types of storage with one copy stored offline.

- *Remember, when securing your backup, you want to act like you are securing your actual data as it will contain everything a malicious actor would want.*

✓ **Have knowledge of what you are backing up.**
Ensure your backups include the systems your business relies on or can't run without, such as financial records, customer databases, etc. Ask yourself whether your business can operate without it.

✓ **Don't forget to test.**
It is important to test your backups and the recommendation is at least quarterly. If you have never tried restoring your backup, then there is no plan in place. Testing backups helps identify incomplete files, long processing times, or password mishaps.

SECURITY PRACTICE #3 Behavioral Monitoring

The Uninvited Guest: Custom malware is on the rise and AI is fueling it.

Malware is short for malicious software and is any program designed to harm your systems, steal your data, or give attackers control of your computer. Ransomware, trojans, worms, and spyware are all types of malware. Defending against modified and custom malware is one of the harder challenges for SMBs, precisely because these threats are designed to slip past the antivirus software that most budget-conscious organizations rely on. A smart, layered defense focuses on what the program is doing, not just what it looks like.

One of the most impactful steps is deploying an endpoint detection and response (EDR) solution rather than a traditional antivirus tool. Modern EDR tools are far more affordable than they used to be and focus on behavioral detection, flagging what a process is doing, as well as identifying known malware signatures. This is critical against custom or modified malware that hasn't been seen before.

In addition, network segmentation is a low-cost, high-impact control that can limit how far an attacker can move if they do get in. Even with a basic managed switch and a consumer-grade firewall, you can isolate critical systems, like your OT, from general user workstations. Custom malware often relies on lateral movement, so separating workstations from operational equipment can make the difference between a minor incident and a full business disruption.

SECURITY PRACTICE #4 Continuous Monitoring

Keep an Eye Out for Trouble: Some adversaries don't break down the door. They slip in and stay awhile.

Most SMBs focus their efforts on keeping attackers out, although that is necessary, it isn't always enough. The average attacker now sits inside a victim's network for weeks or months, meaning the damage is often done long before anyone notices. During that time, they are learning your business, quietly setting up ways to stay in, even if you reboot your computers. This waiting period is called "dwell time," and it is why detection matters as much as prevention. Defending against this requires shifting from a purely preventive mindset to one that includes hunting, even at a reduced scale.

Luckily, the good news is that meaningful monitoring doesn't require a security operations center or a dedicated analyst, you can start by paying attention to what you already have.

- ✓ **Have an endpoint detection and response tool?**
  Use what it is already telling you. The EDR is monitoring across your computers and is only useful when attention is paid to its alerts. Assign someone to review the EDR alerts at least weekly.

- ✓ **Turn on notifications from your accounts.**
  Most business software, such as Microsoft, Google Workspace, QuickBooks, etc., can send you an email or an alert when something unusual happens. Turning these on for admin accounts can help detect logins from new devices, password changes, user additions, and more.

- ✓ **Review access regularly.**
  Most breaches involve accounts that should have been disabled months earlier, so at least once a month, review for the following: admin access to accounts and critical systems, accounts you don't recognize, and former vendors.

- ✓ **Abnormal activity.**
  There are no fancy tools for inherent knowledge of what would be considered abnormal occurrences. Keep an eye out for after-hour logins, which computers talk to your important systems, when vendors use their remote access, etc.

And when you are ready or able, you can always level up or outsource. For example, larger SMBs or those in higher-risk positions may eventually want to centralize logs from all their systems into one place to help search across them during an incident. Businesses can do this by implementing a security information and event management (SIEM) tool. SMB-accessible options exist, offering pay-as-you-go pricing, free tiers, and fully open-source models.

However, for most food and agriculture SMBs, a realistic path is to use a managed service provider (MSP) that provides the tooling, analysts, and response capabilities should something go wrong. MSPs can charge anywhere from $500 - $2,000 per month, depending on size and scope, but it still clocks in cheaper than a full-time security focused employee.

SECURITY PRACTICE #5 Phishing

Spot the Hook: Smell something phishy? Trust your gut.

Despite technological advances that have made cyberattacks more sophisticated, low-tech phishing remains the most common method for cybercriminals to gain access to victims' networks. 65 of the 72 adversaries we tracked leveraged targeted spearphishing attacks. The goal is always the same: to get the victim to click a link or open a file, either stealing their login credentials or installing malicious software on their device.

For food and agriculture businesses, phishing can show up in very familiar ways and typically follows the same playbook - create urgency, impersonate a trusted party or person, and apply pressure so you act before you think. For example:

- A “new” invoice from an equipment dealer or supplier you actually use.
- A text message claiming to be from a driver with a “new” number, asking for an address or schedule.
- An urgent message from a senior-level employee asking for a wire transfer or banking information.

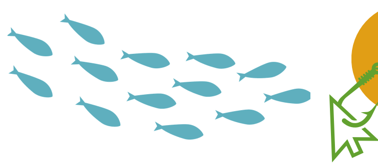
It is important to keep in mind that phishing has spread beyond our email boxes with attackers now reaching out through text messages (smishing), voice calls (vishing), social media, and collaboration tools. With AI becoming more prevalent, the bar for sophistication keeps rising, meaning the old advice of watching for typos and broken grammar can’t be fully reliable.

How to spot the hook:

- **Look for alarming headlines.**
  Attackers tend to use urgent language or impersonate well-known companies to make you act without thinking.
- **Watch for familiar faces.**
  Business email compromise (BEC) is a common form of attack in which attackers impersonate trusted parties or 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.
- **Verify before acting.**
  Whether it is an email, text, or voicemail, and it seems off, treat it as suspicious by default and verify it through another channel. Especially if the request is for anything financial, from wire instructions to banking details.

Remember these important tips to avoid being on the hook for phishing:

- ✓ 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.
- ✓ Always verify the sender's email address, name, and domain.
- ✓ Protect devices by using antivirus, anti-spam, and anti-spyware software.
- ✓ Report phishing emails to the appropriate security or IT staff immediately.



Want to go deeper on phishing?
Read our dedicated blog here.

SECURITY PRACTICE #6 Employee Awareness and Training

Educate Before it's Too Late: Give your team the power to prevent security incidents in their tracks.

Enacting and maintaining a strong cybersecurity posture for your organization begins with your employees, your first line of defense against potential attacks. Employees remain a primary target for threat actors seeking a foothold, and educating your team on cybersecurity best practices can go a long way toward keeping that door closed. According to a 2025 Verizon report, an estimated 60% of security breaches across organizations involve a human element, but organizations that prioritize regular cybersecurity training can significantly reduce that liability risk.

The plus side is that a training program doesn't have to be expensive or time-consuming to be effective, but it needs to be consistent. However, effective training practices go beyond simple videos and multiple-choice quizzes. Organizations should reinforce these lessons year-round through checks, tests, and retraining to ensure their employees keep their skills sharp. Additionally, cybersecurity training programs must evolve regularly to address not only the basics of phishing identification and password security but also modern issues such as deepfakes and AI threats.

Along with ongoing training and education, it is imperative to build a culture in which reporting is not only safe but also encouraged. Employees make mistakes, perhaps they click on a phishing link, but as long as they report it, they should know they are doing the right thing. Employees who hide mistakes can cause more damage. The goal is to create a workplace where the first instinct after a mistake is to tell someone immediately, not hope no one notices.

Though the importance of security awareness training is not unique to the food and agriculture sector, it is one of the easiest and most effective ways to significantly boost your organization's cybersecurity.

SECURITY PRACTICE #7 Disruption and Availability

Disruptive attacks aren't just an inconvenience; they can cause spoiled product, missed shipments, and broken trust.

Some hackers aren't just looking to steal data, they can also want to cause a scene or shut you down. Geopolitical, ideological, and financially motivated threat actors have historically used web defacements and distributed-denial-of-service (DDoS) attacks to inflict additional pain on victims. DDoS attacks are malicious attempts to disrupt a server or network by overwhelming it with a flood of fake internet traffic. These attacks can disrupt business operations, hurt reputations, and distract from the work of managing a business. SMBs should ensure their web applications and CMS platforms are kept rigorously patched, since the overwhelming majority of defacements exploit known, unpatched vulnerabilities rather than novel techniques. Web application firewalls (WAF) can block many of the automated exploit attempts that lead to defacement.

For web defacement specifically, having a tested, clean backup that can be rapidly restored dramatically reduces the business impact. Hosting on a managed platform that handles patching and has built-in rollback functionality can effectively outsource much of this burden at relatively low cost.

For DDoS mitigation, the most practical first step is moving behind a cloud-based scrubbing service. Free tools that offer meaningful volumetric DDoS protection are widely available, even to the smallest organizations.

SECURITY PRACTICE #8 Patch and Software Management

Unpatched = Unprotected. The fix is usually free, but the delay is what costs you.

Food and agriculture organizations employ a wide variety of technologies, including software applications, to assist at every stage of the farm-to-table pipeline. However, even the most robust software can harbor hidden vulnerabilities or introduce exploits, providing an entry point for cybercriminals. The speed at which attackers can exploit these weaknesses is skyrocketing, making vulnerabilities all the more dangerous to leave unaddressed.

Attackers move fast. Once a vulnerability is publicly disclosed, exploits often appear within days (sometimes even hours). For an SMB, the realistic goal isn't to patch everything on day one but to patch the most crucial ones quickly - the "patch first and patch next" approach.

In order to do this, ensure you have an inventory, even a spreadsheet, of the following:

- Every computer, server, and device is connected to your network.
- The operating system and each version it runs.
- What business-critical software is installed on each (accounting, POS, email, etc.)?
- Any "smart" or connected equipment, such as sensors, cameras, thermostats, etc.
- Any vendor-managed system, even though patching is someone else's responsibility.

Companies can maintain regular patch management to ensure that software, firmware, and drivers are consistently hardened against the latest known threats. Enabling automatic updates when possible eliminates or greatly reduces the window of opportunity for attackers. When patches are delayed, organizations should be prepared to implement temporary mitigations or disconnect high-risk systems if necessary. However, it is also a good idea to check your vendors' websites for announcements about available patches and updates.

If a patch or update isn't available yet or can't be installed immediately, if possible, be prepared to isolate the affected machine by temporarily disconnecting it from the internet to keep the rest of your business's network safe.

SECURITY PRACTICE #9 Third Party and Vendor Risk Management

Supply Chain Pain: Attacks don't stop at the source, they spread - causing cascading impacts across the entire sector.

Defending against supply chain attacks starts with knowing what (and who) you're connected to. Supply chain attacks happen when a hacker targets or gains access to a partner or software provider rather than targeting your business directly. That said, it is important to keep an inventory of every third-party vendor, software provider, and service that touches your network or operational systems. This includes everything from your accounting software to seed/equipment suppliers who may have remote access to your systems. You can't protect what you don't know you have, and visibility is free.

Apply the principle of least privilege aggressively. This means tightly limiting vendor remote access to specific times and roles, rather than leaving a permanent open door into your network. Ideally, this access should be routed through a dedicated VPN account or a simple access management tool that lets you revoke their "key" instantly once the job is done. By ensuring that vendor access is disabled as soon as it is no longer needed, you can eliminate a massive amount of risk to your operation without requiring a significant financial investment.

Ask questions of your vendors. Some simple sample questions include:

- **Do you use MFA internally?**
  → *Answer should be yes!*
- **Have you had a breach in the last two years?**
  → *If the answer is yes, ask for the incident report.*
- **Is your product secure by default? If so, what does that entail? If not, what is automatically "turned on" for us?**
  → *This will help you understand what steps you will need to take to secure the product once it is delivered to you.*

Additional questions to consider can be found in the IT-ISAC's Critical SaaS SIG whitepaper on shared responsibility.

Lastly, stay informed by subscribing to your vendor alerts, news providers, and other services like CISA's Known Exploited Vulnerabilities catalog. These services can be free and offer early warning to your business.

SECURITY PRACTICE #10 Multi-Factor Authentication (MFA) and Credential Security

Adding Another Layer: Require more than just a password and 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. In today's threat landscape, complex passwords are only the baseline, many organizations are moving towards the heightened security of passphrases and utilizing encrypted password managers to keep their digital footprint truly locked down.

Research by Microsoft reported that using MFA can block more than 99.9% of account compromise attacks. That means, beyond passwords, passphrases, and password managers, organizations should also enable multi-factor authentication (MFA) for any accounts that support it. MFA acts as an essential secondary barrier, requiring not just what you know (a password) but something you have (such as a smartphone app or a physical security key). 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.

Not all MFA is created equal though and knowing what to choose from is important:

- **SMS Text or Email Codes**
  Sending a code to your email or phone is the entry-level step in MFA; it is better than no MFA at all, but it should be avoided when stronger options exist.

- **Authenticator Apps**
  Microsoft Authenticator, Google Authenticator, and others generate a code directly on your device that is never transmitted and accessible via an app.

- **Push Notifications**
  Typically faster to use than an authenticator app, it pushes an "approval" screen that you must tap to approve. A recommended option would be the ability to do number matching, in which you have to type a number shown on a screen rather than just tapping a button.

- **Hardware Security Keys**
  Known as the gold standard, these are physical keys that must be present to log in. This type of access is strongly recommended for admin accounts.

Cybercriminals are generally opportunistic, bypassing hardened systems in favor of easier targets. By layering MFA over your accounts, you transform a simple entrance into a high-security vault. MFA is an easy and exceedingly cost-effective way for food and agriculture businesses to increase defenses against attackers.

CONCLUSION

Cybersecurity is not a problem reserved for large enterprises, it is a challenge every organization in the food and agriculture sector faces, regardless of size. For SMBs, the stakes are just as high - a single incident can disrupt operations, erode customer trust, and send ripple effects across the supply chain.

The good news? You don't have to solve it all at once. The practices in this guide are practical, affordable, and impactful. Implementing even a handful of them puts you meaningfully ahead of where most attackers expect you to be. Threat actors are largely opportunistic. The harder you make yourself to compromise, the more likely they are to move on.

Cyber defense is not a destination, it is an ongoing commitment. The threat landscape will keep evolving, and so should your defenses. It is important to stay curious and stay informed. Every effort, no matter how big or small, helps to make your organization and the sector a safer place for all. And always, remember to lean on resources like the Food and Ag-ISAC to keep pace with what is emerging in the sector. In this industry, we're all connected — and we defend better when we defend together.

The Food and Agriculture - Information Sharing and Analysis Center (Food and Ag-ISAC) was built by industry for industry as a collaborative community. By bringing companies together to share threat intelligence, analysis, and effective security practices, the Food and Ag-ISAC helps members detect attacks, respond to incidents, and exchange indicators - strengthening protection and risk management across their organizations and the sector.

Learn more at foodandag-isac.org.
Email us at membership@foodandag-isac.org.