



FOUNDED 2000

Food and Ag Cybersecurity:

A Guide for Small & Medium Enterprises



May 2023

ABOUT THE IT-ISAC

Founded in 2000, the Information Technology-Information Sharing and Analysis Center (IT-ISAC) is a non-profit organization that augments member companies' internal capabilities by providing them access to curated cyber threat analysis, an intelligence management platform, and a trusted forum to engage with senior analysts from peer companies.



ABOUT THE FOOD AND AG-ISAC

The IT-ISAC originally established the Food and Agriculture Special Interest Group (SIG) in 2013 to help what was then a small number of member companies in the industry protect their enterprise. Now as the Food and Ag-ISAC, we will continue to help food and agriculture companies identify attacks, incidents, threat indicators, and effective mitigation strategies so they can better protect their enterprise and the sector.



IT-ISAC FOOD AND AG INDUSTRY BOARD MEMBERS



FOLLOW US ON SOCIAL!



INTRODUCTION

The Food and Agriculture sector faces both common and distinctive cybersecurity challenges. The industry leverages information technology in the same way other industries do for core business and administrative functions. But it also uses technology in unique ways, such as in processing plants, farm equipment, precision agriculture, and product storage and transfer. Likewise, the industry faces a range of threat actors such as targeted nation-state activity, organized criminal campaigns, and social activists. Companies in the industry can also be unintended or random victims of cyberattacks not targeting them or the industry specifically.

Given the interconnected nature of the industry, it is important that companies of all sizes take appropriate steps to secure their technology environments. While cybersecurity is often viewed as an issue for “big companies,” small and medium-sized businesses tend to be at a greater risk since they often lack the resources and expertise to effectively mitigate cyber threats. Because of this, small and medium-sized businesses are often targeted by threatening adversaries.

This guide details cost-effective steps that small and medium-sized companies can take to help protect themselves. No company, no matter the size, is immune from cyber risk. Implementing these practices will not guarantee protection from a breach, but they can help to reduce the likelihood of being breached. These practices will also increase your ability to respond effectively and successfully should an attack or breach occur.

There is an Appendix at the end of this guide that uses *Ransomware* as a case study to show how applying these security practices can help defend organizations against one of the most disruptive types of cyberattacks facing enterprises today. However, the purpose of this guide is to help companies improve their cybersecurity, not just protect themselves from ransomware. While we use *Ransomware* as a case study, companies should begin with a comprehensive security approach, rather than trying to defend against specific threats. As such, we encourage companies to implement the below list of effective security practices and then add capabilities as needed.

EFFECTIVE SECURITY PRACTICES FOR SMALL AND MEDIUM-SIZED ENTERPRISES

While no company or network is impenetrable from attack, there are a series of effective practices that companies can take to manage risks to their enterprises. Many of these can be implemented for no or relatively low cost. Applying these security practices can reduce the likelihood that your company will become a victim of a successful attack and increase the chance your company will recover if it is a victim of a cyberattack.

Security Practice #1: Update Your Software

Much like armies look for vulnerabilities in opposing forces, attackers look for vulnerabilities in a target's network. It is common for vendors to issue "patches" or updates to plug vulnerabilities in their hardware or software as they are discovered. Organizations should work to patch systems and software vulnerabilities as soon as possible once patches are available. 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 #2: Use Unique Passwords

Reusing the same password(s) for multiple accounts can jeopardize all accounts, even if only one account is compromised. The [National Institute of Standards and Technology \(NIST\)](#) recommends the use of unique passwords that contain a combination of at least 8 letters, numbers, and special characters.

Password managers are an effective tool for easily managing multiple unique passwords. With a password manager, you can create individualized passwords that are difficult to guess, while still having coherence and being easy to manage. If a hacker gains access to one account, they won't be able to use the same password to access other accounts. It's also important to keep your passwords secure by not sharing them with anyone, or put in a place where they can easily be found.

Security Practice #3: Deploy Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) provides added protection in case someone acquires (or guesses) an account's password. MFA 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 is better.

Security Practice #4: Backup Files

Ensuring access to your files is essential for business continuity should your organization suffer an attack or otherwise be forced offline. Backing up essential files and data in real-time helps ensure business continuity. Online backup systems are easy to use but can be costly depending on the amount of data you have. In some cases, there are plenty of quality low-cost commercial online backup services. Since some cyberattacks target online backups it is important to keep an offline version in the event your online storage is compromised. Backups should always be encrypted.

Your backups are only as good as your backup processes. If you don't backup your files often, you may have to restore to a previous date that lacks recent files. It also is important to check the backup software on occasion to ensure that it is working properly.

Security Practice #5: Encrypt Sensitive Files

Remember not all information is equal. Some of your information is more important or sensitive than others. Deploy encryption to protect your most sensitive information and documents, including customer information, Personally Identifiable Information (PII), and emails.

Security Practice #6: Segment Your Networks

This will limit risk to the operational networks and minimize risk to those operations if there is a disruption to the corporate networks. To the extent possible, limit internet connections to your operational technologies. If they must be connected, ensure operational networks such as manufacturing and production are segmented from business networks. Organizations can reduce this risk by identifying links between business and production environments and developing segmentation to continue operations should one network fall to a cyber event. By separating business and operational networks, organizations can avoid operational disruptions should the corporate IT be impacted by a cyber incident.

Security Practice #7: Don't Take the Bait

One of the most common ways attackers breach networks is by enticing someone to click on a malicious link. Attackers often send “phishing” emails with suggestive headings or impersonating recognizable company names that contain malware. The goal is to get the victim to click on a link or file, which will then download malicious software on the machine.

To avoid becoming a victim:

- Do not open emails or download software from untrusted sources.
- Do not click on links or attachments in emails that come 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.

Sometimes the attackers impersonate a trusted party or have compromised a known contact. If the email seems “phishy” or suspicious or you are uncertain, call (do not email) the person to confirm the email is authentic.

Security Practice #8: Do not Connect to Public Wi-Fi Networks

Public Wi-Fi networks should always be treated as insecure. Since anyone can access a public network, threat actors can use tools to monitor and intercept data from other users on the network. If you must connect to a public Wi-Fi network, always use a Virtual Private Network (VPN) solution to encrypt your communications. You can also use a password protected personal hotspot instead of a public Wi-Fi network. Insecure communications on public Wi-Fi channels could result in the theft of sensitive information.

Security Practice #9: Develop and Test a Response Plan

An incident response plan is important not just to address the immediate incident, but also to ensure the organization can survive the impact of an attack. Companies should consider how you would respond if your company became the victim of a cyberattack.

- Who would you call for assistance?
- What customers or partners would you notify?
- When do you engage with your attorney?

Documenting a response plan and practicing it will help you respond more quickly and effectively.

Security Practice #10: Engage with Your Peers

Talk to your employees, peers, and partners about cybersecurity. Share information about threats you are seeing so they can be better prepared and ask what they are seeing so you can be better prepared. Share this guide with your employees and peers to make them aware of how they can protect their company. Let your employees know you take cybersecurity seriously and expect them to do so as well. Every employee is a critical part of your security team and often your first line of defense.

APPENDIX: Ransomware Case Study

Ransomware is a type of attack in which an attacker gains access to a network and installs malware that encrypts or locks files so that an individual or organization can no longer rely on or access them. The threat actor will demand the victim to pay a ransom (often in cryptocurrency) to unlock the files. Attackers frequently threaten to make public the information they have stolen if payment is not made. However even when a victim makes ransomware payments, attackers do not always unlock or release the data. In these cases, the attacker now has both the victim's data and their money.

Ransomware is one of the most high-profile attacks used by nation-states and cybercriminals. Although law enforcement has had increased success in disrupting ransomware attacks, organizations are victimized by these attacks every day. Ransomware attacks are common across all industries, including the food and agriculture industry. As long as the risk of getting caught is low and the likelihood of making money is high, these campaigns will continue.

These attacks can be highly disruptive and can shut down business operations for days or weeks. Responding to them is complex, time intensive, and expensive. Making ransomware payments can also violate federal law if payments are made to organizations that are sanctioned by the U.S. government.

The following are steps organizations can take to help avoid the disruption, the pain, and the expense from a ransomware attack.

Security Practice #1: Update Your Software


Vulnerable software products are a common initial access vector for ransomware actors. These actors weaponize vulnerabilities within hours of their disclosure and it does not take long for limited attacks to become widespread. By keeping your software up to date, you reduce the number of vulnerable points on your network, making it harder for ransomware actors to find an initial entry point.

Security Practice #2: Use Unique Passwords

If a malicious actor were to gain access to your account or networks, they could encrypt your files and prevent you from accessing them. If an actor were to obtain or guess the password to one account, they could gain entrance to all accounts. The ransomware actor will then have access to everything. By using unique passwords for all your accounts, you can avoid exposing multiple accounts to cyberattacks.

Security Practice #3: Deploy Multi-Factor Authentication (MFA)

While passwords are necessary, they are not always sufficient. Ransomware actors often use legitimate credentials to carry out attacks. Cybercriminals have easy access to stolen or compromised credentials. Some are purchased from a third-party service known as an initial access broker. Enabling multi-factor authentication (MFA) can prevent ransomware actors who have your account password from gaining access to both your account and network if they have your account password.



60% of small businesses go out of business within six months of a cyberattack.*

*Statistic from <https://www.verizon.com/business/resources/articles/small-business-cyber-security-and-data-breaches/>

Security Practice #4: Backup Files

If you were to be a victim of a ransomware attack, you will want to recover as quickly and efficiently as possible. Having a backup of your files and data that you can restore will help you to continue operations as you respond to the incident. Online backups enable data to be backed up in real-time. In some cases, ransomware will target cloud-based backup solutions rendering them useless. Therefore, offline backup solutions provide additional redundancy for worse-case scenarios. Ensure you perform backups frequently, so they remain current.

Security Practice #5: Encrypt Sensitive Files

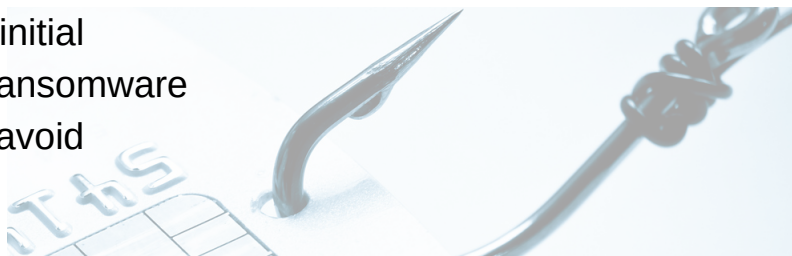
By encrypting your most sensitive files, you can protect your information from cybercriminals should it be stolen in an attack. Many ransomware actors will steal your files before encrypting them. If files are encrypted correctly, the stolen files are inaccessible to ransomware actors, which will make leaking them useless and of no value to the attacker.

Security Practice #6: Segment Your Networks

In some cases, ransomware attacks may be focused on disrupting business operations at a plant or other key facility as an incentive for the victim to pay the ransom. Segmenting corporate business functions from manufacturing and production operations is one way to reduce this risk. This prevents a malware incursion on one network from bleeding over into others.

Security Practice #7: Don't Take the Bait

Phishing remains one the most common initial access point for cyberattacks, including ransomware attacks. Employees should be trained to avoid common phishing scams.



Security Practice #8: Develop and Test a Response Plan

Having a ransomware specific response plan in place can help you recover and restore operations more quickly. Some of the questions your response plan should answer include, but are not limited to:

- How will you restore encrypted files on your network?
- How will you communicate to your customers?
- How will you determine what data was accessed by the cybercriminals?
- How will you engage with law enforcement and third-party service providers to help you recover from the attack?
- How do you determine if you will pay the ransom?
- If you are going to pay, do you know how to buy cryptocurrency?
- How do you contact your cyber insurance company?

Security Practice #9: Engage with Your Peers

Ransomware groups are sharing information within their enterprises and with threat actors to be more successful. They are learning from each other to improve their capabilities and be more effective. In the same way, network defenders must collaborate and learn from each other. There are different ransomware actors with different tactics, techniques, and procedures (TTPs). The actors and their TTPs change. Engaging with peer companies can help you stay informed of this changing landscape so you can better defend.



Food Ag ISAC

An IT ISAC Community

RESOURCES

- Cybersecurity & Infrastructure Security Agency
 - [Cross-Sector Cybersecurity Performance Goals](#)
 - [Multi-Factor Authentication Fact Sheet](#)
- National Institute of Standards and Technology
 - [Cybersecurity Framework](#)
 - [Password Guidance](#)

Food and Ag-ISAC
9401 Centerville Road, Suite 104
Manassas, VA 20110

FOODANDAG-ISAC.ORG

