March
2026

INSIDER THREAT TO THE FOOD AND AGRICULTURE SECTOR

JOB AID

CDSE Center for Development of Security Excellence

INTRODUCTION

What Is Insider Threat?

An insider threat is anyone with authorized access who uses that access to wittingly or unwittingly harm the organization or its resources. Insiders can include employees, vendors, partners, suppliers and others that you provide access to your facilities and/or information. Most insider threats exhibit risky behavior prior to committing negative workplace events. If identified early, many threats can be mitigated before harm to the organization occurs. Learn more about insider risk indicators and find free training and awareness materials here.

What Threats do Insiders Pose to Food and Agriculture?

Numerous threats have the potential to cause major disruption in food and agriculture operations and to harm public health and safety. These include malicious acts committed by insiders such as deliberate food adulteration, fraud, theft, sabotage, and workplace violence. Unwitting insiders may inadvertently disclose proprietary or sensitive information, impact food safety through negligent actions, or unknowingly download malware or facilitate other cybersecurity events. The food and agriculture sector is also vulnerable to transportation and supply chain failures, contamination, and threats to industrial control systems or other technical systems. Unmitigated insider risk is likely to increase these vulnerabilities.

What You Need to Know

As a member of the Food and Agriculture Sector, you play a significant role in national security by protecting public health and safety, the nation, and its economy from contamination, economic espionage, food adulteration, and terrorism.

Trusted insiders, both witting and unwitting, can cause grave harm to your organization's facilities; resources including raw materials, finished products, and information; brand, reputation, and personnel. Insider incidents account for billions of dollars annually in actual and potential damages related to food safety, food defense, tampering, terrorism, trade secret theft, fraud, sabotage, damage to an organization's reputation, acts of workplace violence, and more.

Implementation of an Insider Risk Mitigation Program can help address risks associated with trusted insiders. Click the links to learn how to establish an Insider Risk Program at your organization and develop a risk management strategy that addresses areas critical to food and agriculture.

INSIDER THREATS: A DIRECT THREAT TO FOOD

The Food and Agriculture sector, a cornerstone of societal well-being and economic stability, faces an increasingly complex and insidious threat landscape. While external attacks garner significant attention, the risk posed by malicious or negligent insiders often remains underappreciated. Insider threats, stemming from disgruntled employees, compromised individuals, or simply negligent personnel, can manifest in a variety of devastating ways, ranging from intentional food contamination and theft of proprietary information to sabotage of critical infrastructure and the facilitation of crippling cyberattacks. The interconnectedness of the modern food supply chain, coupled with the sector's increasing reliance on technology, creates numerous vulnerabilities that insiders can exploit, potentially with catastrophic consequences for public health, the environment, and the global economy. Understanding the diverse nature of these insider threats, their motivations, and the potential impacts is paramount for organizations seeking to protect their operations, reputation, and ultimately, the safety and security of the food supply.

- **Key takeaway:** The Food and Agriculture sector faces significant insider threats, often underestimated compared to external attacks.
- **Types of Threats:** Ranging from food contamination and IP theft to infrastructure sabotage and cyberattacks.
- **Underlying Factors:** Interconnected supply chains and increasing reliance on technology create vulnerabilities.
- **Potential Impacts:** Catastrophic consequences for public health, the environment, and the global

This Job Aid provides a comprehensive overview of the multifaceted nature of insider threats within the Food and Agriculture sector. It explores the various forms these threats can take, from deliberate acts of sabotage to unintentional security breaches caused by human error. It delves into specific examples of how insiders can exploit vulnerabilities in physical security, data protection, and operational protocols, resulting in significant financial losses, widespread reputational damage, and potentially devastating impacts on public health.

THREATS TO OUR FOOD AND AGRICULTURE

A. Intentional Food Contamination: A Recipe for Disaster

One of the most alarming and potentially devastating insider threats is the intentional contamination of food products. A malicious actor, whether a disgruntled employee, an individual driven by extremist motives, someone who has been bribed, or even an activist seeking to make a statement, could introduce harmful substances into the food supply. This could involve adding bacteria (e.g., Salmonella, E. coli), chemicals (e.g., pesticides, cleaning agents, poisons), or foreign objects (e.g., metal shards, glass, plastic) to food products at any stage of the production process, from initial ingredient sourcing to packaging and distribution. The intent could range from causing minor disruption and financial harm to the company, to inflicting widespread illness, injury, or even death. The motivations behind such an act are diverse and complex, making prevention and detection challenging.

Example:

In a National Library of Medicine article an analysis of 76 intentional food adulteration events between 2009 and 2022 revealed they caused over 250 deaths and nearly 5,000 illnesses. The most severe incidents occurred during the manufacturing stage, accounting for over 80% of deaths, with the primary motives being economic gain or revenge. The study highlights that perpetrators often had legitimate access to the food, although they remained unidentified in many cases. Intentional Adulteration of Foods with Chemicals: Snapshot for 2009–2022

Vulnerabilities Exploited

- **Weak Physical Security:** Inadequate perimeter security (e.g., unlocked doors, broken fences), unrestricted access to production areas, insufficient controls over who can enter specific areas, lack of controlled access points, and ineffective visitor management.
- **Insufficient Background Checks and Screening:** Failing to conduct thorough background checks on new hires, neglecting to re-screen employees periodically, overlooking red flags during the hiring process, and not performing psychological evaluations or substance abuse screenings where appropriate.
- **Poor Food Safety Protocols and Procedures:** Lax adherence to HACCP (Hazard Analysis and Critical Control Points) principles, inadequate employee training on food safety and hygiene, lack of robust testing procedures, ineffective sanitation practices, and insufficient documentation and record-keeping.
- **Lack of Video Surveillance and Monitoring:** Absence of comprehensive video surveillance coverage, blind spots in critical areas, inadequate retention policies for video footage, and failure to actively monitor surveillance feeds.
- **Inadequate Internal Controls and Reporting Mechanisms:** Lack of anonymous reporting systems for employees to raise concerns, failure to investigate reported issues thoroughly, insufficient auditing of food safety procedures, and absence of a clear chain of command for addressing potential threats.

- **Disgruntled Employees and Poor Morale:** Ignoring signs of employee dissatisfaction, failing to address grievances promptly, creating a hostile work environment, and not providing opportunities for career advancement.
- **Supply Chain Vulnerabilities:** Lack of visibility and control over the entire supply chain, including ingredient sourcing, transportation, and storage. Reliance on untrusted or unverified suppliers.

B. Theft of Proprietary Information: Stealing the Seeds of Innovation

In the intensely competitive Food and Agriculture sector, intellectual property (IP) such as advanced seed formulas, proprietary growing techniques (e.g., precision agriculture methods, optimized fertilization schedules), unique and protected recipes (e.g., for sauces, flavorings, processed foods), and even sophisticated equipment designs can be incredibly valuable. This IP represents years of investment in research and development, market analysis, and brand building. An insider, motivated by financial gain, revenge, or ideological reasons, could steal this information through various means and sell it to a competitor, provide it to a foreign government, or even use it to launch a competing business. This unauthorized disclosure gives the recipient an unfair advantage, undermines the company's innovation pipeline, and can have far-reaching negative consequences.

Example:

As an employee of a Chinese conglomerate, Mo Hailong, a/k/a Robert Mo participated in a long-running conspiracy to steal genetically modified inbred corn seeds from DuPont Pioneer and Monsanto test fields in Iowa and Illinois. DOJ, U.S. Attorney's Office, Southern District of Iowa (Oct. 2016)

Vulnerabilities Exploited:

- **Weak Access Controls:** Inadequate role-based access control (RBAC), allowing employees to access sensitive data beyond their job responsibilities. Lack of multi-factor authentication (MFA) for accessing critical systems. Failure to regularly review and update access privileges.
- **Lack of Data Loss Prevention (DLP) Measures**: Absence of DLP tools to monitor and prevent the exfiltration of sensitive data via email, file sharing, USB drives, and cloud storage services. Ineffective content filtering and data classification policies.
- **Inadequate Employee Monitoring**: Insufficient monitoring of employee computer activity, network traffic, and data access patterns. Failure to detect unusual or suspicious behavior. Lack of audit trails for data access and modification.
- **Insufficient Protection of Digital Assets:** Weak encryption of sensitive data at rest and in transit. Inadequate security measures for protecting servers, databases, and other critical infrastructure. Lack of regular vulnerability assessments and penetration testing. Failure to implement robust patch management processes.
- **Weak Physical Security of Data Storage:** Unsecured server rooms, poor control over access to data storage devices, and a lack of procedures for securely disposing of outdated hardware.
- **Ineffective Security Awareness Training:** Failing to educate employees about the risks of data theft and the importance of protecting intellectual property. Lack of training on recognizing and reporting phishing attempts and social engineering attacks.
- **Lack of Non-Disclosure Agreements (NDAs) and Intellectual Property Agreements:** Failure to have robust NDAs and IP agreements in place with employees, contractors, and partners. Insufficient enforcement of these agreements.
- **Cloud Security Weaknesses:** Misconfigured cloud storage settings, inadequate security controls for cloud-based applications, and insufficient monitoring of cloud activity.
- **Poorly Defined Data Ownership:** Lack of clarity regarding data ownership and responsibility, leading to confusion and potential security gaps.

C. Sabotage of Equipment or Systems: Crippling Our Ability to Produce

Our food production and agricultural operations are critically dependent on a complex network of interconnected equipment and systems running smoothly and reliably. A malicious insider, motivated by factors such as revenge, financial gain (e.g., being paid by a competitor), or ideological opposition to the company's practices, could intentionally damage, disable, or misconfigure critical equipment, thereby causing significant production delays, substantial financial losses, potential food safety risks, and damage to the company's reputation. This sabotage could involve physically tampering with machinery, corrupting software systems, disrupting communication networks, or manipulating environmental controls. The intent is to disrupt or halt operations, cause economic harm, or potentially endanger public health.

Example:

Ravi Kumar Chermala, the former Director of Quality Assurance for Kerry Inc., has pleaded guilty to three misdemeanor charges of introducing adulterated food into interstate commerce. His plea is connected to a 2018 Salmonella outbreak linked to Kellogg's Honey Smacks, a cereal produced at a Kerry facility he oversaw, and was sentenced to one year of probation in June 2023. DOJ Office of Public Affairs (Oct. 2022)

The company also agreed to pay a criminal fine and forfeiture amount totaling $19.228 million. If the guilty plea is accepted by the court, the $19.228 million fine and forfeiture will constitute the largest-ever criminal penalty following a criminal conviction in a food safety case. DOJ Office of Public Affairs (Feb. 2023)

Vulnerabilities Exploited:

- **Lack of Physical Security Controls:** Weak perimeter security around critical infrastructure, insufficient access control to equipment rooms and control panels, unattended equipment, and inadequate monitoring of personnel activity in sensitive areas. Failure to secure equipment against unauthorized physical access (e.g., using locks, tamper-evident seals).
- **Inadequate System Monitoring:** Insufficient real-time monitoring of equipment performance, network traffic, and system logs. Lack of anomaly detection capabilities to identify unusual or suspicious activity. Failure to establish baseline performance metrics to identify deviations that indicate potential sabotage.
- **Disgruntled Employees:** Poor employee morale, unresolved grievances, lack of communication, and a hostile work environment. Failure to identify and address warning signs of potential insider threats (e.g., unusual behavior, expressed resentment).
- **Insufficient Backup Systems and Redundancy:** Lack of redundant systems to maintain operations in the event of equipment failure or sabotage. Inadequate backup power supplies and emergency generators. Failure to regularly test backup systems to ensure their functionality.
- **Weak Cybersecurity Posture:** Vulnerable industrial control systems (ICS) and SCADA systems that can be remotely accessed and manipulated. Insufficient security measures to protect against malware infections and unauthorized access to critical systems. Lack of regular security audits and penetration testing.
- **Poor Configuration Management:** Inconsistent or poorly documented configurations of equipment and systems, making it difficult to detect unauthorized changes. Lack of change management procedures to track and approve modifications to critical systems.
- **Inadequate Training and Awareness:** Insufficient training for employees on how to identify and report suspicious activity. Lack of awareness among employees about the potential consequences of sabotage.
- **Legacy Systems and Unpatched Vulnerabilities:** Reliance on older, unsupported equipment or software with known vulnerabilities. Failure to apply security patches and updates in a timely manner.
- **Poor Vendor Security:** Reliance on third-party vendors for equipment maintenance and support without adequate security oversight. Lack of security requirements in vendor contracts.

D. Facilitating a Cyberattack: Opening the Door to Digital Disaster

Cyberattacks represent an increasingly sophisticated and pervasive threat to the Food and Agriculture sector, as highlighted by both the Cybersecurity and Infrastructure Security Agency (CISA) and leading cybersecurity resources like CybersecurityGuide.org. These attacks can disrupt operations, compromise sensitive data, and cause significant financial and reputational damage. While external threats are a major concern, a critical, often overlooked, vulnerability lies within the organization itself: the insider threat. An insider, whether acting unintentionally through negligence or intentionally through malicious intent, can significantly facilitate a cyberattack. This could involve actions such as clicking on a deceptive phishing link, inadvertently sharing their login credentials with unauthorized individuals, intentionally disabling security controls, or even planting malware within the network. The consequences can range from minor disruptions to catastrophic breaches that cripple entire organizations. The Food and Agriculture sector is particularly vulnerable due to its reliance on outdated systems, limited IT security expertise, and the critical nature of its infrastructure, which makes it a prime target for ransomware attacks.

Example:

A former technician in South Carolina, William Jason Taylor, is facing federal charges for allegedly manipulating a poultry plant's chemical cleaning systems in August 2023. Prosecutors allege he remotely altered levels of hazardous sanitizing chemicals and disabled safety alarms, leading to six counts of unauthorized computer access. Taylor was sentenced to six months in federal prison on November 4th, 2023. The case highlights the significant vulnerability of the nation's automated food supply chain to cybersecurity breaches and insider threats. PennState College of Agricultural Science (May. 2025)

Vulnerabilities Exploited:

- **Lack of Employee Training and Awareness:** Insufficient or infrequent security awareness training programs that fail to educate employees about phishing scams, social engineering tactics, malware threats, and best practices for password security. Failure to conduct regular phishing simulations to test employee awareness and identify areas for improvement.
- **Weak Password Policies:** Lack of strong password policies that enforce the use of complex passwords, regular password changes, and multi-factor authentication (MFA) for all critical systems and accounts. Failure to prohibit the reuse of passwords across multiple accounts.
- **Inadequate Email Security:** Ineffective email filtering and anti-spam solutions that fail to block phishing emails and malicious attachments. Lack of email encryption to protect sensitive data transmitted via email. Failure to implement Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting & Conformance (DMARC) to prevent email spoofing.

- **Insufficient Intrusion Detection and Prevention Systems:** Lack of robust intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor network traffic for malicious activity and block cyberattacks in real time. Failure to configure IDS/IPS systems properly or to keep them up-to-date with the latest threat intelligence.
- **Poor Patch Management:** Failure to apply security patches and updates to software and operating systems in a timely manner, leaving systems vulnerable to known exploits. Lack of a centralized patch management system to automate the patching process.
- **Inadequate Endpoint Security:** Lack of endpoint detection and response (EDR) solutions to protect workstations, laptops, and mobile devices from malware and other cyber threats. Failure to implement application whitelisting to prevent unauthorized software from running on endpoints.
- **Weak Network Segmentation:** Lack of network segmentation to isolate critical systems and prevent the spread of malware throughout the network. Failure to implement firewalls to control network traffic between different segments.
- **Privileged Access Management (PAM) Deficiencies:** Inadequate controls over privileged accounts, allowing users to access systems and data beyond their legitimate needs. Failure to implement the principle of least privilege, which limits user access to only the resources necessary to perform their job duties.
- **Lack of Incident Response Planning:** Absence of a comprehensive incident response plan that outlines procedures for responding to cyberattacks, including steps for containment, investigation, and recovery.
- **Unsecured Remote Access:** Allowing remote access to the network without adequate security measures, such as VPNs and multi-factor authentication. Failure to monitor remote access activity for suspicious behavior.
- **Use of Outdated Systems:** Reliance on older, unsupported operating systems and software that lack security updates and are vulnerable to known exploits.

E. Supply Chain Disruption: Breaking the Chain That Feeds Us

The Food and Agriculture supply chain is a highly complex and interconnected network, spanning from farm to table and involving numerous stakeholders, including producers, processors, distributors, retailers, and consumers. This intricate web presents multiple opportunities for disruption. An insider, whether a disgruntled employee, a saboteur acting on behalf of a competitor, or an individual coerced or bribed by an external actor, could intentionally disrupt this critical chain by manipulating shipping records, deliberately delaying deliveries, diverting shipments to unauthorized locations, tampering with temperature controls during transportation, or even compromising the integrity of tracking systems. Such actions can have devastating consequences, potentially leading to widespread shortages, significant economic losses, food spoilage and waste, and damage to public trust in the food system.

Example:

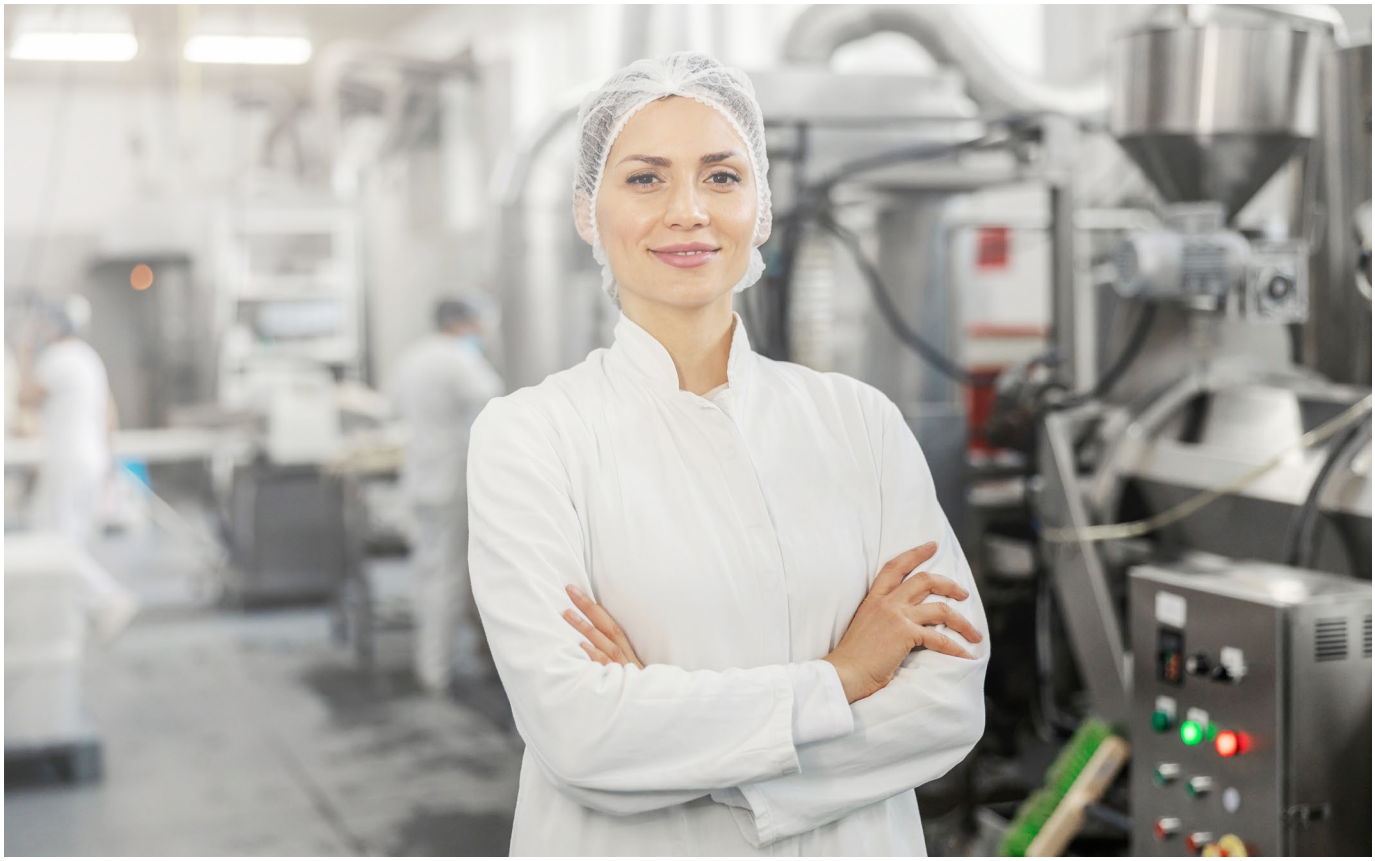
Sayee Chaitanya Reddy Devagiri, a former DoorDash driver, has pleaded guilty to federal wire fraud for his role in a scheme that stole over $2.5 million from the company. He admitted to using employee credentials to manipulate DoorDash's software, creating a rapid cycle of fake deliveries that he and co-conspirators would claim for payment. As the third defendant to be convicted in the conspiracy, Devagiri was sentenced to 21 months in prison on February 10th, 2026. U.S. Attorneys Northern District of California Press Releases (May 2025)

Additional Reading: Members Of Conspiracy To Steal More Than $2.5 Million

Vulnerabilities Exploited:

- **Lack of Supply Chain Security Controls:** Insufficient security protocols and procedures to monitor and protect the integrity of the supply chain. Absence of a comprehensive supply chain risk management framework.
- **Inadequate Employee Screening and Background Checks:** Failing to conduct thorough background checks on employees with access to sensitive supply chain data and critical infrastructure. Neglecting to re-screen employees periodically to identify potential risks.

- **Weak Access Controls:** Lack of robust access controls to prevent unauthorized access to shipping records, inventory management systems, and other critical supply chain data. Inadequate role-based access control (RBAC) principles.
- **Insufficient Monitoring of Shipments:** Inadequate real-time tracking and monitoring of shipments throughout the supply chain. Lack of anomaly detection capabilities to identify suspicious deviations from planned routes or delivery schedules.
- **Lack of Supply Chain Visibility:** Limited visibility into the operations of suppliers, distributors, and other partners in the supply chain. Insufficient data sharing and communication between stakeholders.
- **Poor Physical Security at Storage and Transit Locations:** Weak security measures at warehouses, distribution centers, and transportation hubs, making it easier for insiders to tamper with goods or manipulate records.
- **Inadequate Cybersecurity Measures:** Vulnerabilities in transportation management systems (TMS), warehouse management systems (WMS), and other critical software applications used to manage the supply chain.
- **Lack of Business Continuity Planning:** Absence of robust business continuity plans to mitigate the impact of supply chain disruptions. Insufficient redundancy and backup systems to ensure continued operations in the event of an incident.
- **Poor Communication and Coordination:** Lack of clear communication channels and coordination between different stakeholders in the supply chain, making it difficult to respond effectively to disruptions.
- **Over-Reliance on Single Suppliers:** A concentration of reliance on a small number of suppliers. If one supplier is compromised, the entire chain is disrupted.



POTENTIAL IMPACTS TO OUR FOOD SUPPLY CHAIN

Consolidated List of Potential Impacts from Insider Threats in the Food and Agriculture Sector:

This list represents a comprehensive overview of the potential consequences that can arise from various insider threats affecting the Food and Agriculture sector. The impacts are categorized for clarity.

I. Direct Impacts on Human Health and Safety:

- **Widespread Illness, Injury, and Death:** Potential for mass casualties due to contaminated food products, malicious cyberattacks affecting food safety systems, or sabotage of critical equipment. This is the most severe potential outcome.
- **Foodborne Illness Outbreaks:** Increased risk of foodborne illness outbreaks due to contamination, mislabeling, or compromised temperature controls.
- **Potential Harm to Consumers:** Distribution of contaminated or unsafe food products to consumers, leading to illness, injury, or death. This includes risks to individuals with allergies due to intentional allergen contamination.

II. Financial and Economic Impacts:

- **Significant Financial Losses:** This encompasses a broad range of financial impacts, including:
  - Reduced sales, decreased profits, and increased operating costs.
  - Costs associated with product recalls, system recovery, ransomware payments, and legal fees.
  - Loss of investment in research and development (due to theft of intellectual property).
  - Increased security costs (due to the need to improve security measures after an incident).
  - Equipment repair and replacement costs (from sabotage).
  - Increased waste disposal costs (from food spoilage).
  - Increased insurance premiums.
  - Potential regulatory fines and penalties.
- **Production Delays and Shutdowns:** Significant disruptions to production schedules, leading to missed deadlines, lost revenue, and potential for complete shutdowns of operations.
- **Supply Chain Disruptions:** Interruptions to the flow of raw materials and finished products, leading to shortages, increased prices for consumers, and negative impacts on other businesses in the supply chain.

- **Food Spoilage and Waste:** Loss of perishable goods due to temperature fluctuations, equipment malfunctions, delays in transportation, or contamination.
- **Economic Impact on the Community and Region:** Job losses, business closures, and reduced economic activity in areas heavily reliant on the affected food production facilities.
- **Loss of Competitive Advantage:** Erosion of market share as competitors gain access to proprietary information, disrupt operations, or launch similar products/services.
- **Increased Food Prices:** Supply chain disruptions and production inefficiencies can drive up food prices, making it more difficult for consumers to afford nutritious food.
- **Economic Instability:** Major disruptions can have significant economic consequences, particularly for rural communities and developing countries.

III. Reputational and Legal Impacts:

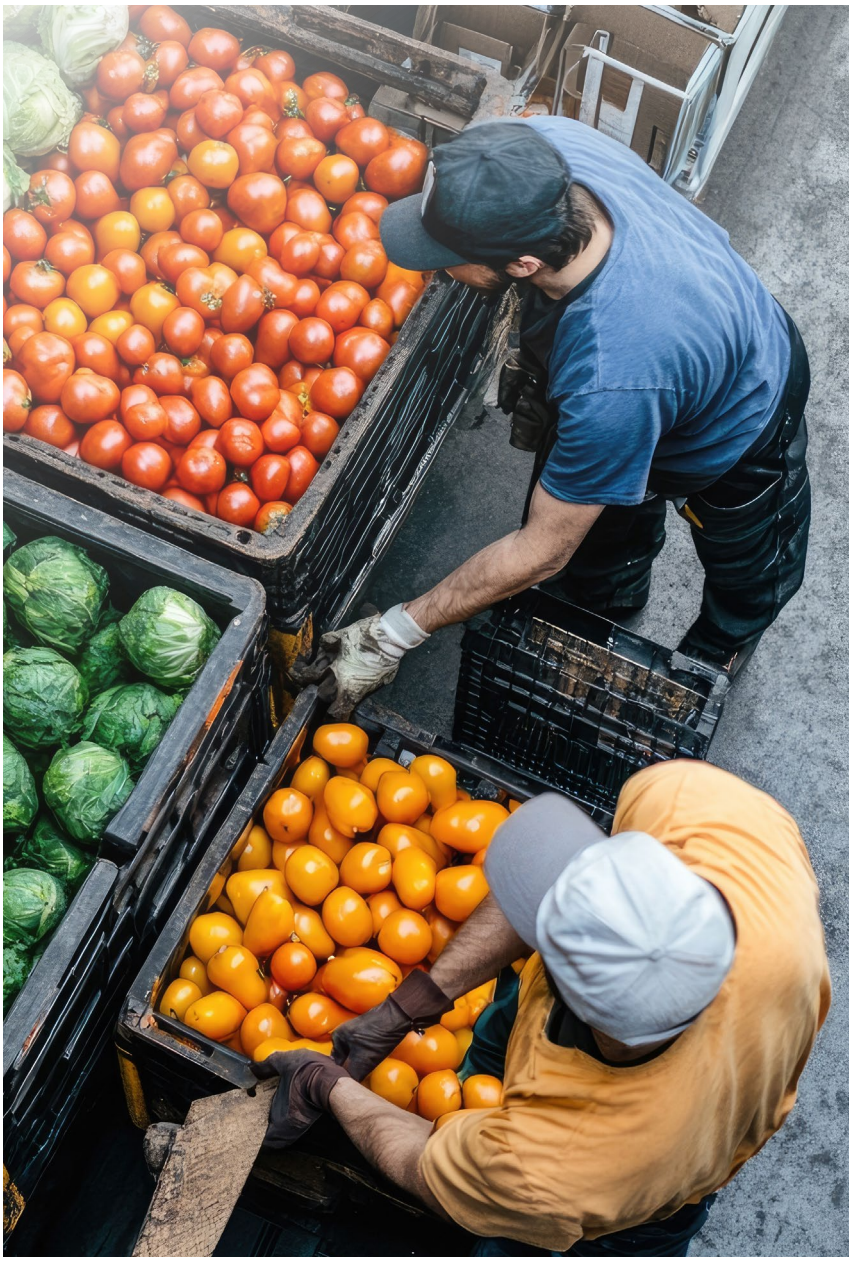
- **Reputational Damage:** Erosion of consumer trust, loss of investor confidence, and damage to the company's brand image, leading to decreased sales, market share, and long-term brand value erosion.
- **Legal Battles and Liability:** Costly and time-consuming legal disputes over intellectual property rights, trade secrets, patent infringement, product liability, or regulatory violations.
- **Potential Criminal Charges and Legal Liability:** Criminal prosecution for individuals involved in illegal activities and potential civil lawsuits against the company.
- **Increased Regulatory Scrutiny and Oversight:** Increased inspections, stricter regulations, and more frequent audits from government agencies.
- **Regulatory Penalties:** Fines and penalties from government agencies for violations of food safety regulations, data privacy laws, environmental laws, and other applicable regulations.
- **Damage to the Company's Long-Term Viability:** Undermining the company's ability to innovate, compete effectively, and maintain a sustainable business model.

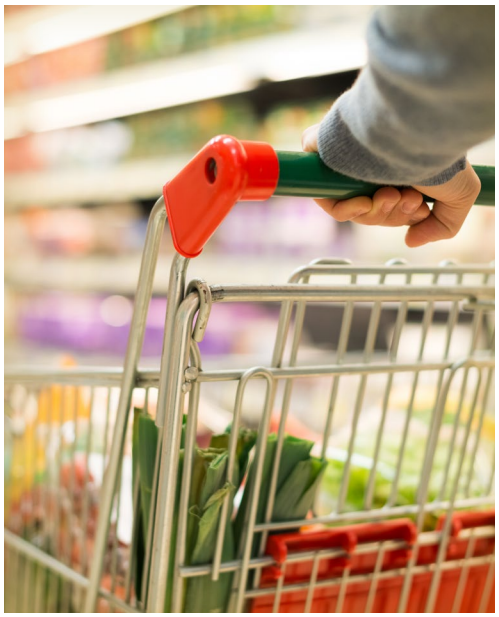
IV. Operational and Technological Impacts:

- **System Downtime:** Disruption of critical systems and services, leading to production delays, supply chain disruptions, and loss of revenue.
- **Compromise of Industrial Control Systems (ICS):** Attacks on ICS can disrupt or disable critical infrastructure, such as irrigation systems, temperature controls, automated processing lines, and food safety monitoring equipment.
- **Data Breaches:** Unauthorized access to sensitive data, including customer information, financial records, trade secrets, and intellectual property.
- **Operational Disruption:** Disruption to farming operations, food processing, distribution, and other critical functions.
- **Loss of Intellectual Property:** Theft of valuable intellectual property, such as seed formulas, growing techniques, proprietary recipes, and equipment designs.
- **Counterfeit Products and Product Diversion:** Stolen information can be used to create counterfeit products that are sold at lower prices, further damaging the company's brand and eroding market share. Legitimate products may also be diverted into unauthorized channels.
- **Environmental Damage:** Equipment malfunctions or intentional acts can lead to environmental contamination from chemical spills, leaks, or unauthorized discharges.

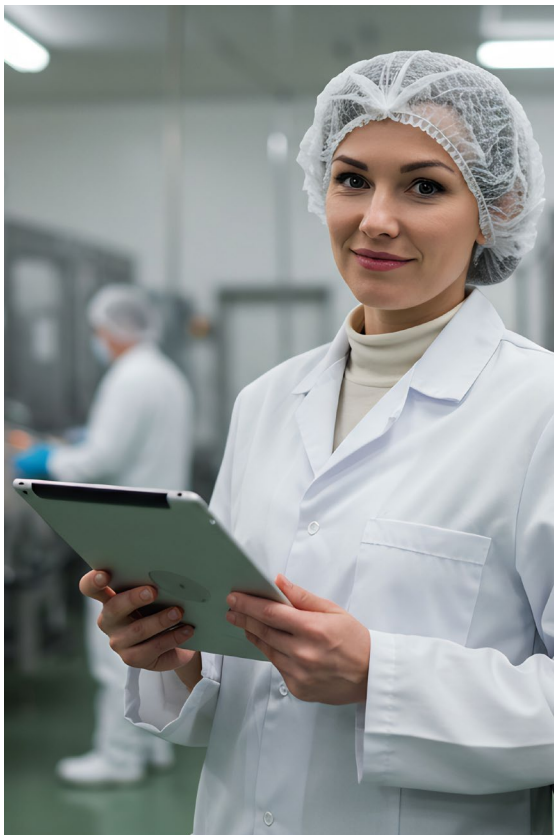
V. Broader Societal Impacts:

- **Erosion of Public Confidence in the Food System:** Undermining consumer trust in the safety and security of the food supply, leading to widespread anxiety and fear.
- **Potential Shortages of Food Products:** Disruption to the food supply chain can lead to shortages of essential food products, particularly in remote or vulnerable communities.
- **Geopolitical Instability:** In extreme cases, supply chain disruptions can lead to social unrest and political instability, particularly in regions that are heavily reliant on food imports.
- **Economic Espionage:** Stolen information can be used by foreign governments or competitors to gain an unfair economic advantage, potentially harming the company and the national economy.





MITIGATION STRATEGIES



I. Foundational Security Measures (Applicable Across All Threat Categories):

- **Conduct Thorough Background Checks and Screening:** Perform comprehensive background checks, pre-employment screenings, and periodic re-screenings for all employees, contractors, and vendors, especially those with access to sensitive information, critical infrastructure, or food production processes.
- **Implement Robust Access Controls:** Enforce strict role-based access control (RBAC) and the principle of least privilege. Regularly review and update access privileges. Utilize multi-factor authentication (MFA) for all critical systems and accounts. Revoke access immediately upon termination of employment.
- **Provide Comprehensive Security Awareness Training:** Conduct regular, engaging, and tailored security awareness training for all personnel. Cover topics such as phishing, social engineering, malware, data handling, physical security, reporting procedures, and ethical conduct. Use simulations and practical exercises to reinforce learning.
- **Develop and Enforce Strong Security Policies:** Establish clear, well-defined security policies and procedures covering all aspects of operations, including data handling, password management, acceptable use of technology, physical security, and incident reporting. Ensure these policies are readily accessible and consistently enforced.
- **Implement Robust Physical Security Measures:** Secure facilities with perimeter security (fences, lighting, surveillance), access control systems (badges, biometrics), and security personnel. Restrict access to sensitive areas (production floors, storage facilities, server rooms). Implement visitor management procedures.
- **Foster a Culture of Security:** Promote a culture of security awareness and responsibility throughout the organization. Encourage employees to report suspicious activity without fear of reprisal. Establish clear channels for reporting concerns and provide avenues for anonymous reporting.
- **Regular Security Audits and Risk Assessments:** Conduct regular security audits and risk assessments to identify vulnerabilities and weaknesses in systems, processes, and procedures.
- **Incident Response Planning:** Develop and regularly test comprehensive incident response plans that outline procedures for responding to various security incidents, including data breaches, cyberattacks, sabotage, and food contamination events.
- **Secure Remote Access:** Implement secure remote access solutions with VPNs, multi-factor authentication, and strong password policies. Monitor remote access activity for suspicious behavior.
- **Establish Vendor Security Management:** Implement a vendor security management program to assess and manage the security risks associated with third-party vendors. Include security requirements in vendor contracts and conduct regular audits of vendor security practices.

II. Data and Information Security:

- **Implement Data Loss Prevention (DLP) Solutions:** Deploy DLP tools to monitor and prevent the unauthorized exfiltration of sensitive data. Implement content filtering and data classification policies.
- **Encryption:** Encrypt sensitive data at rest and in transit. Use strong encryption algorithms and manage encryption keys securely.
- **Data Backup and Recovery:** Implement a comprehensive data backup and recovery plan. Store backups offline and in a secure location. Regularly test backup and recovery procedures.
- **Secure Data Disposal:** Implement procedures for securely disposing of sensitive data and hardware.

III. Cybersecurity Specific Measures:

- **Endpoint Detection and Response (EDR):** Deploy EDR solutions on all endpoints (workstations, laptops, servers) to detect and respond to malware and other cyber threats.
- **Intrusion Detection and Prevention Systems (IDS/IPS):** Implement IDS/IPS systems to monitor network traffic for malicious activity and block cyberattacks.
- **Patch Management:** Implement a centralized patch management system to automate the patching of software and operating systems. Regularly scan for vulnerabilities and prioritize patching efforts.
- **Network Segmentation:** Segment the network to isolate critical systems and prevent the spread of malware. Use firewalls to control network traffic between segments.
- **Email Security:** Implement robust email filtering and anti-spam solutions. Enforce the use of email encryption. Implement SPF, DKIM, and DMARC.
- **Web Filtering:** Implement web filtering to block access to malicious websites and prevent the download of malware.
- **Vulnerability Management:** Conduct regular vulnerability scans and penetration testing to identify weaknesses in systems and applications.

IV. Food Safety and Operational Security:

- **Implement Robust Food Safety Programs:** Develop and implement comprehensive food safety programs based on HACCP principles. Ensure proper employee training, sanitation practices, and testing procedures.
- **Establish Redundancy and Backup Systems:** Implement redundant systems to maintain operations in the event of equipment failure or sabotage. Install backup power supplies and emergency generators.
- **Temperature Monitoring:** Implement continuous temperature monitoring systems for perishable goods.
- **Supply Chain Visibility:** Improve supply chain visibility through data sharing and communication protocols with suppliers, distributors, and other partners. Implement real-time tracking and monitoring of shipments.
- **Diversify Suppliers:** Reduce reliance on single suppliers by diversifying the supply base. Identify alternative sources of supply.
- **Business Continuity Planning:** Develop comprehensive business continuity plans to mitigate the impact of disruptions.
- **Configuration Management:** Implement a centralized configuration management system for critical equipment and systems.
- **Anomaly Detection:** Implement anomaly detection systems to identify unusual activity in food production processes and supply chains.
- **Secure Industrial Control Systems (ICS):** Implement robust security measures to protect ICS and SCADA systems from cyberattacks. Segment ICS networks and implement strong access controls.

V. Human Resources and Personnel Management:

- **Employee Assistance Programs (EAPs):** Provide access to EAPs to support employees struggling with personal issues.
- **Address Employee Morale and Grievances:** Create a positive work environment, address employee grievances promptly, and promote open communication.
- **Regular Performance Reviews:** Conduct regular performance reviews to identify potential issues and provide feedback to employees.

VI. Legal and Regulatory Compliance:

- **Enforce Non-Disclosure Agreements (NDAs) and Intellectual Property Agreements:** Ensure that all employees, contractors, and partners sign robust NDAs and IP agreements. Enforce these agreements rigorously.
- **Comply with Relevant Laws and Regulations:** Comply with all relevant laws and regulations related to food safety, cybersecurity, and data privacy.

ADDITIONAL RESOURCES

2025-2026 Insider Threat Vigilance Campaign - CDSE

Cyber Insider Threat - CDSE (eLearning Course)

Cybersecurity Attacks - CDSE (The Insider Threat Short)

Potential Risk Indicators: Insider Threat - CDSE (Job Aid)

Insider Threat Indicators in User Activity Monitoring - CDSE Insider Threat Toolkit

Taking Culture Seriously - CDSE (Webinar)

Food and Agriculture Defense - Department of Homeland Security (DHS)

Food and Agriculture Sector - Cybersecurity & Infrastructure Security Agency (CISA)

Recovery from Food or Agriculture Incidents - Federal Emergency Management Agency (FEMA)

Food Defense Risk Mitigation Tool - United States Department of Agriculture (USDA)

Insider Risk Management Program Office - U.S. Department of Commerce

Best Practices in Cyber Supply Chain Risk Management - National Institute of Standards and Technology (NIST)

Insider Threat Mitigation Resources and Tools - Cybersecurity & Infrastructure Security Agency (CISA)