

INSIDER THREAT DIVISION

CENTER FOR DEVELOPMENT OF EXCELLENCE

FOOD DEFENSE CONSORTIUM

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

CDSE



INSIDER RISK AWARENESS



**Rebecca Morgan, Chief, Insider Threat Division
Center for Development of Security Excellence
Defense Counterintelligence and Security Agency**

INSIDER RISK AWARENESS



- **I Don't Need an Insider Threat Program**
- **It's Too Difficult to Establish an Insider Threat Program**
- **I Don't Have the Expertise to Run an Insider Threat Program**
- **I Can't Afford an Insider Threat Program**

INSIDER RISK AWARENESS



Defining Insider Threat

Insider

Anyone with authorized access.

INSIDER RISK AWARENESS



Defining Insider Threat

Insider Threat

The likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to an organization, including the loss or compromise of information, facilities, and personnel.

INSIDER RISK AWARENESS



Defining Insider Threat



INSIDER RISK AWARENESS



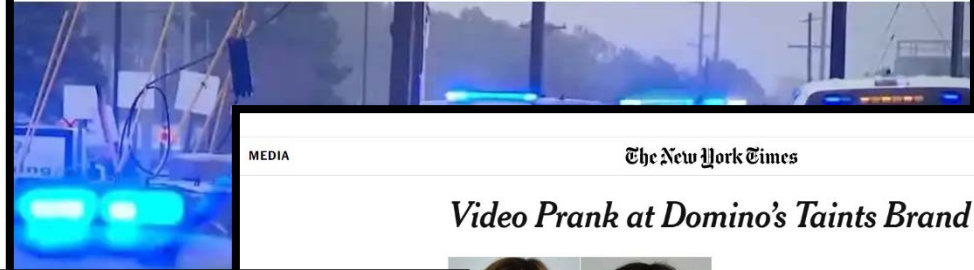
Insider Threats in Food and Agriculture Sector

- Food Adulteration
- Contamination
- Data Breach
- Fraud
- Theft
- Sabotage
- Loss of Trade Secret or Proprietary Data
- Tainted Supply Chains
- Acts of Violence

Report: One person shot at food service plant in Georgia, search for shooter

by Gary Detman | Friday, December 13th 2019

AA



MEDIA

The New York Times

Video Prank at Domino's Taints Brand



Online comments helped the police identify Kristy Hammonds and Michael Setzer as the makers of a troubling kitchen video. Photographs from the Conover, N.C., Police Department

Stephanie Clifford

15, 2009



When two Domino's Pizza employees filmed a prank in the restaurant's kitchen, they decided to post it online. In a few days,

The Chinese spy in the Iowa corn field



Award-winning ears of corn are displayed at the Iowa State Fair in Des Moines last August. A Chinese company sent operatives to Iowa to pick up genetically modified corn seeds and send them to China, so scientists there could reverse-engineer their own corn varieties. (John Taggart/Bloomberg)

By Dina Temple-Raston

Dina Temple-Raston is a long-time correspondent for NPR and was the host and creator of "I'll Be Seeing You," an NPR series of radio specials that looked at the technologies that watch us. She is the author of four books, including "The Jihad Next Door: The Lackawanna Six and Rough Justice in the Age of Terror."

March 6, 2020 at 8:00 a.m. EST

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

Witting and Unwitting Insiders



INSIDER RISK AWARENESS



Factors Contributing to Vulnerability

Access

Potential
Risk
Indicators

Perceived
Life Crisis

Opportunity and crisis contribute to vulnerability.

INSIDER RISK AWARENESS



Potential Risk Indicators (PRIs)

Most employees engaging in negative behavior showed one or more PRIs.

- ☐ Access Attributes
- ☐ Professional Lifecycle and Performance
- ☐ Foreign Considerations
- ☐ Security and Compliance Incidents
- ☐ Technical Activity
- ☐ Criminal, Violent, or Abusive Conduct
- ☐ Financial Considerations
- ☐ Substance Abuse and Addictive Behaviors
- ☐ Judgement, Character, and Psychological Conditions



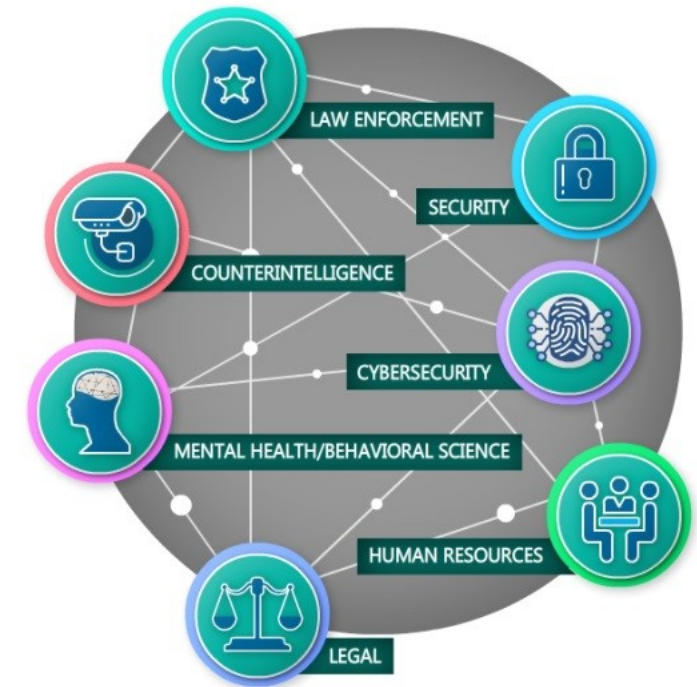
**See something,
say something!**

INSIDER RISK AWARENESS



Insider Risk Programs

- ☐ **Multidisciplinary** Teams
- ☐ **Proactively** Deter, Detect, and Mitigate Risk
- ☐ Respect the **Privacy** and Civil Liberties of the Workforce
- ☐ Seek **Positive** Outcomes
- ☐ Manage Risk to **Protect** Organizations and their Resources



INSIDER RISK AWARENESS

Resources



INSIDER RISK AWARENESS



ESTABLISH your insider risk program by working with senior leadership to designate a senior official or program manager. Work with senior managers from throughout your company including security, human resources, legal, and information technology representatives to craft an Insider Risk Program Plan and establish information sharing policies and mitigation strategies. Conduct a Risk Assessment to identify critical assets, threats to your organization, unique vulnerabilities, and appropriate countermeasures to address the insider threat.

DETER insider threat activities and manage insider risk by instituting training and awareness programs for all personnel. Ensure that principles of organizational trust, fairness, and transparency are part of your work culture and communicated to employees. Evaluate work processes and security protocols such as pre-employment vetting, principle of least privilege, separation of duties, and termination procedures to ensure that insider risk considerations are in place.

DETECT behaviors and activities indicative of potential risk by encouraging reporting to front line managers, supervisors, human resources, security and insider risk program personnel. Consider establishing designated email and/or phone lines and ensure employees know what to report and to whom. Establish user activity monitoring capability on sensitive systems or those that house proprietary data.

INSIDER RISK AWARENESS



MITIGATE potential risk by addressing insider risk indicators early – before a negative event occurs. Coordinate with your multidisciplinary insider risk team to deploy proactive interventions. Many risks can be mitigated with increased training, updated security protocols, or human resources and employee assistance program strategies. Decide how the team will handle indicators and ensure fair, consistent application of mitigation strategies.

REFER insider threat incidents and/or potential risk indicators that cannot be resolved to appropriate local and federal law enforcement. Make sure employees know to call 911 when there is a threat of imminent danger.

MATURE your insider risk program over time by conducting self-assessments to determine the effectiveness of your deterrence, detection, and mitigation capabilities. Consider insider threat specific training for insider risk team personnel and coordinate with partners in your industry to identify best practices. Engage with federal agencies and organizations for access to resources.



INSIDER RISK AWARENESS



Insider Risk Job Aid

Insider Risk Programs for the Food and Agriculture Sector

IMPLEMENTATION GUIDE



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

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

Implementation of an Insider Risk Program can help mitigate 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.

[Understanding Insider Risks](#)[Establishing an Insider Risk Program](#)[Insider Risk Management Strategy](#)[Insider Risk Program Resources](#)

CDSE Center for Development of Security Excellence

UNDERSTANDING INSIDER RISKS

WHAT IS INSIDER RISK?
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 threat-related risks behave prior to committing negative workplace events. If identified early, many risks can be mitigated before harm to the organization occurs. Learn more about insider risk indicators and food loss training and awareness materials [here](#).

WHAT RISKS DO INSIDERS POSE TO FOOD AND AGRICULTURE?
Insiders threaten the potential to cause severe disruption to food and agriculture operations and to harm public health and safety. These include malicious acts committed by insiders such as deliberate food adulteration, food theft, sabotage, and workplace violence. Unintentional insider acts may unintentionally disclose proprietary or sensitive information, impact food safety through negligent actions, or inadvertently forward malware or facilitate other cyber-related threats. The food and agriculture sector is also vulnerable to supply chain hijacking, contamination, and threats to industrial control systems or other regulated systems. Unintentional insider risk is likely to increase their vulnerability. Click [here](#) to learn about insider risk indicators on the food and agriculture sector.

WHY ESTABLISH AN INSIDER RISK PROGRAM?
Insider Risk Programs are designed to detect, deter, and mitigate the risks associated with trusted insiders. Understanding "insider" is the cornerstone of security, business resilience, cyber, legal and operational. From identifying your organization's goals, strategies, and capabilities to understanding the potential risk and damage exposure mitigation options, as a case by case basis. Most of these exposures are not unique to your organization and can be managed. Insider Risk Programs also protect the privacy of the employees while reducing potential harm to the organization. See the [Link to the Insider Risk Program section](#) to learn more.

HOW CAN MY ORGANIZATION MANAGE INSIDER RISK?
Effective Insider Risk Programs deploy risk management strategies that identify the assets at risk, the potential identity of potential threats, determine vulnerabilities, assess risk and deploy countermeasures. Many countermeasures are as low cost as the organization and insider training and awareness, clear reporting policies, managing organizational trust, and robust security practices. Review the [Insider Risk Management Strategy](#) to learn more.

WHAT RESOURCES ARE AVAILABLE TO ME?
The USDA, FDA, Defense Counterintelligence and Security Agency, Department of Homeland Security, National Insider Threat Task Force, Federal Bureau of Investigation, and the National Counterintelligence and Security Center have resources. See [Insider Threat Resources](#) to learn more.

Food Industry ICS may be distinctly vulnerable to cyberattacks from Insider Threats
Mitigating More Than Just The Cyber Risk To Food Processing and Agriculture: The Department of Homeland Security's Food Protection and Defense Institute (FDPI) is a leading authority on food safety and security. The FDPI is a multi-agency effort that brings together the food industry and specific industrial control system vulnerabilities related to systems, ICS, and data. The FDPI is a multi-agency effort that brings together the food industry and specific industrial control system vulnerabilities related to systems, ICS, and data. The FDPI is a multi-agency effort that brings together the food industry and specific industrial control system vulnerabilities related to systems, ICS, and data.

[RETURN TO MAIN PAGE](#)

ESTABLISHING AN INSIDER RISK PROGRAM

SETTING UP YOUR PROGRAM

- An Insider Risk Program is a multi-disciplinary activity or "task" established by an organization to gather, analyze, and assess information for insider risk detection and mitigation. Program personnel analyze information and activity indicators of insider risk and determine appropriate mitigation response options up to and including referral to the appropriate officials for investigation and/or resolution. Best practices encourage the Insider Risk Program to include multidisciplinary team members of Legal Counsel, Security, Cybersecurity, Human Resources, and Information Systems, and Human Resources or Human Capital Discipline to effectively ensure insider risk in your organization. The exact makeup of your Insider Risk Program will depend on the size and complexity of your organization. Consult the [Insider Risk Guide](#) for more on setting up your organization.
- Insider Risk Programs take proactive measures to detect, deter, mitigate, and report threats associated with trusted insiders. The program identifies individuals who may indicate an individual poses a risk. Early identification allows Insider Risk Program personnel to focus on an individual's cycle of concern or threat and deploy appropriate mitigation responses. When necessary, the team shares relevant information from each discipline with organizational leadership to facilitate timely, informed decision-making and report information outside the organization as required.
- The first step in establishing your program is to identify the program's goals and leadership. You must determine how the team will be structured and where it will be located. Does your organization have the ability to house the team in a single location? Or, are the team members geographically dispersed and must rely on virtual communications to conduct operations? Your organization should select an Insider Risk Program Senior Leader or program manager that oversees day-to-day operations. They will work with the organization's senior leadership to determine resources and staffing needs.
- You should establish rules for how the Insider Risk Program will operate within your organization. As part of risk and policy development, the Insider Risk Program should also identify processes for categorizing sensitive personal information along with compliance with the violations of internal rules established by Insider Risk Programs team members. Insider Risk was designed to meet standards of professional conduct like any other organizational function. Insider Risk Program personnel should be held to the same standards of professional conduct as any other employee. See the [Link to the Insider Risk Program section](#) to learn more.
- You should also ensure that Insider Risk Program personnel are properly trained to conduct their duties. Insider Risk Program personnel must be able to appropriately respond to insider reporting, protect privacy and civil liberties, report mitigation options, and make matters as required. Many food training options exist. Consult the [Insider Risk Guide](#) for more information.

[RETURN TO MAIN PAGE](#)

INSIDER RISK RESOURCES

Insider Risk Program Resources

- Sample Forms
 - Insider Risk Program Plan
 - Insider Risk Program Memorandum of Action
- Training for Insider Risk Programs
 - ICSI
 - DIIS
- Awareness Materials
 - Case Studies
 - Policies and Best Practices
- Supporting Organizations
 - Department of Homeland Security - DHS
 - US Department of Agriculture
 - US Food and Drug Administration
 - National Insider Threat Task Force
 - Defense Counterintelligence and Security Agency - DCSSA

Insider Risk Security Mobile Application available on Apple App Store or Google Play

[RETURN TO MAIN PAGE](#)

Sample Insider Risk Program Plan

1. Purpose. This plan establishes policy and assigns responsibilities for the Insider Risk Program (IRP). The IRP will seek to establish a secure operating environment for personnel, facilities, information, equipment, networks, or systems from insider threats. An insider threat is defined as the individual, risk or potential risk to an organization that is an authorized access, wittingly or unwittingly to the harm to organization not in resources. Insider threats are not limited to the organization's information, personnel and facilities.

The program will gather, analyze, and report relevant and credible information indicative of potential insider risk indicators, drive insider threat, and deter risks posed by those with authorized access to any organizational resources to include personnel, facilities, information, equipment, networks, or systems. The program will proactively mitigate the risk of an insider threat as defined above.

2. Scope and applicability. This Insider Risk Program Plan applies to all staff offices, regions, and personnel with access to any organizational resources to include personnel, facilities, information, equipment, networks, or systems.

3. Guiding Principles

- The IRP will be established to protect personnel, facilities, and information systems from insider risks. This program will seek to protect that. Food, savings, acts of violence, and the loss of intellectual property, proprietary information or other sensitive information. The program will actively deter trusted insiders from becoming insider threats. The program will establish the capability to detect insider who pose a risk to information resources and information. The program will mitigate risks to the organization through collaborative actions, referrals to law enforcement as appropriate, or other responses.
- The IRP will follow identified best practices for insider risk programs and abide by the laws, policies, and regulations of federal, state, and federal governments to appropriate.
- The responsibilities outlined below are designed to enable the IRP to gather, analyze, identify, and respond appropriately to key threat-related information. The IRP will consult with security management and legal counsel to ensure no legal, privacy, civil rights, and civil liberties issues (including but not limited to, the use of personally identifiable information) are appropriately addressed.

4. Responsibilities

- Insider Risk Program Senior Official (IRPSO), will be designated in writing and will act as the company's representative for IRP implementing activities.
- The IRPSO will be responsible for the daily operations, management, and ensuring compliance with the



INSIDER RISK AWARENESS

AWARENESS MATERIALS AT WWW.CDSE.EDU

CASE STUDY
KINETIC VIOLENCE – A Positive Outcome

WHAT HAPPENED

Christopher Paul Hasson was arrested on February 15, 2019, which prevented him from possibly carrying out acts of violence. His arrest followed a multi-year investigation that included monitoring the use of his U.S. Government automated information system. He pleaded guilty in October 2019, and on January 31, 2020, at the U.S. District Court in Greenbelt, MD, was sentenced to 160 months in prison on four federal counts, to include three felony weapons charges and one felony drug charge. Hasson owned a residence in Silver Spring, MD, and worked at the U.S. Coast Guard Headquarters in Washington, D.C.

Hasson self-identified as a "White Nationalist" for over 30 years in writings advocating for "focused violence" in order to establish a white homeland. Review of Hasson's email accounts, saved documents, and text messages, and internet searches revealed he was inspired by uncontrolled assault weapons, studied violence, and considered those he considered

Christopher Paul Hasson

- US Coast Guard Lieutenant
- Former USMC and Army National Guardman
- Secret Clearance (Declined TS//SI)
- No previous derogatory information
- Acquisitions
- 49 years old
- married with children

Turning People Around, Not Turning Them In. S1/E1: "An odd encounter with Tim"

Home / Training / Security Training Videos / Turning People Around, Not Turning Them In, S1/E1: "An odd encounter with Tim"

Susan has an odd encounter with Tim at the office. Watch the video and put yourself in her shoes. What would you do, and why?

The Insider Threat Vigilance Video Series adds the workforce in identifying and reporting insider threat indicators. The series also provides an overview of Insider Threat Programs and their multi-disciplinary approach to gathering and reviewing information indicative of an insider threat, referring that data as appropriate, and developing mitigation response options all while protecting the privacy and civil liberties of the workforce. The goal of the program is to detect threats and detect potential issues early on before a problem occurs. Click the links to learn more...

Episode 1 - "An odd encounter with Tim" Season One: Turning People Around, Not Turning Them In

Watch later

Watch

The Critical Pathway. S2/E1: "Organizational Trust"

Home / Training / Security Training Videos / The Critical Pathway. S2/E1: "Organizational Trust"

The Insider Threat Vigilance Video Series adds the workforce in identifying and reporting insider threat indicators. In this second season, an unexpected change needs uncertainty. How does leadership handle the change? Click the links to learn more...

The Critical Pathway - Episode 1: "Organizational Trust"

Watch

Think

Dig Deeper

Question

Welcome to the game of Whodunit.

Your organization has experienced a major data leak. Important secret information has somehow gotten into the hands of a competitor or adversary. It's up to you to figure out who did it, how, and where it happened.

Study the first scenario shown on the next page to learn what happened. Then get to know the possible suspects, location where the incident may have occurred, and potential methods used to obtain the data. When you think you know the answer, go ahead and make an accusation! But hurry, you must identify the source of the leak and mitigate the damage.

There are seven mysteries. Some are easy to solve. Click the green arrow to move to the next incident.

Whodunit

Insider Threat Awareness Trivia Twirl

SPIN THE WHEEL

Reporting

User Activity Monitoring

Collection Methods

Indicators

Infamous Insiders

Want to start the game over?

[Learn how to play.](#)

SELF-DISCOVERY IN CRISIS SHOWS STRENGTH.

Be confident in your ability to cope with negative events.

Resilient insiders are less likely to become threats.

JUST BECAUSE IT'S ON THE STREET, DOESN'T MEAN YOU SHOULD TWEET!

TOP SECRET

SHARING CLASSIFIED INFORMATION WITH THE PUBLIC IS #UNAUTHORIZED

CDSE

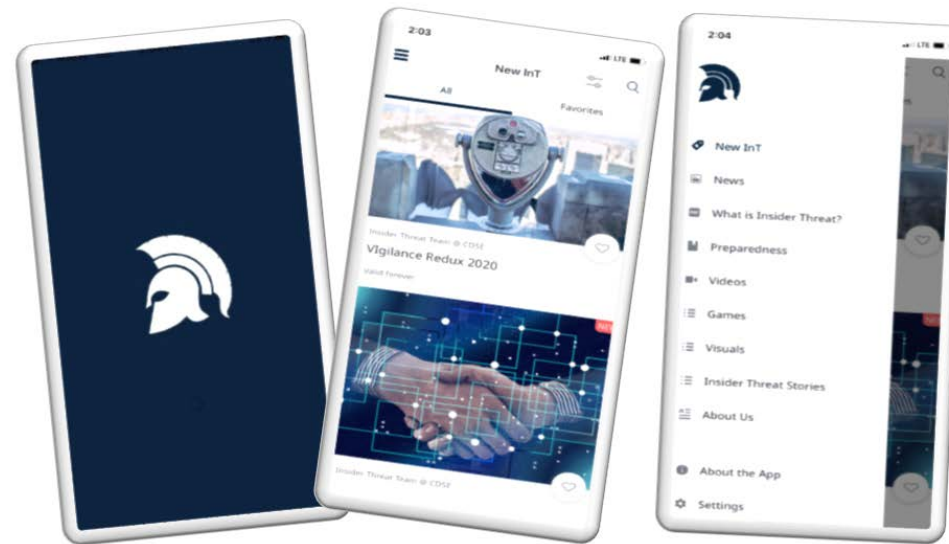
www.cdse.edu

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

INSIDER RISK AWARENESS



Insider Threat Sentry - Mobile Application



RESOURCES



DHS CISA

<https://www.cisa.gov/insider-threat-mitigation>

National Counterintelligence and Security
Center/National Insider Threat Task Force

<https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf>

Defense Counterintelligence and Security Agency

<https://www.dcsa.mil/>

US Department of Agriculture

<https://www.usda.gov/>

Food and Drug Administration

<https://www.fda.gov/home>

FBI

<https://www.fbi.gov/investigate/counterintelligence>

WHERE TO FIND US



CDSE Center for Development of Security Excellence
Education • Training • Certification • Resources •

<https://www.cdse.edu/>

You Tube
<http://www.youtube.com/user/dsscdse>

f <http://tinyurl.com/3p6ghle>

Twitter
[@InT_Aware](#)
[@TheCDSE](#)

Insider Threat Sentry on Apple App Store and Google Play



<https://www.cdse.edu>



INSIDER RISK AWARENESS



Questions?

Rebecca Morgan
Insider Threat Division Chief, CDSE, DCSA
rebecca.a.morgan22.civ@mail.mil