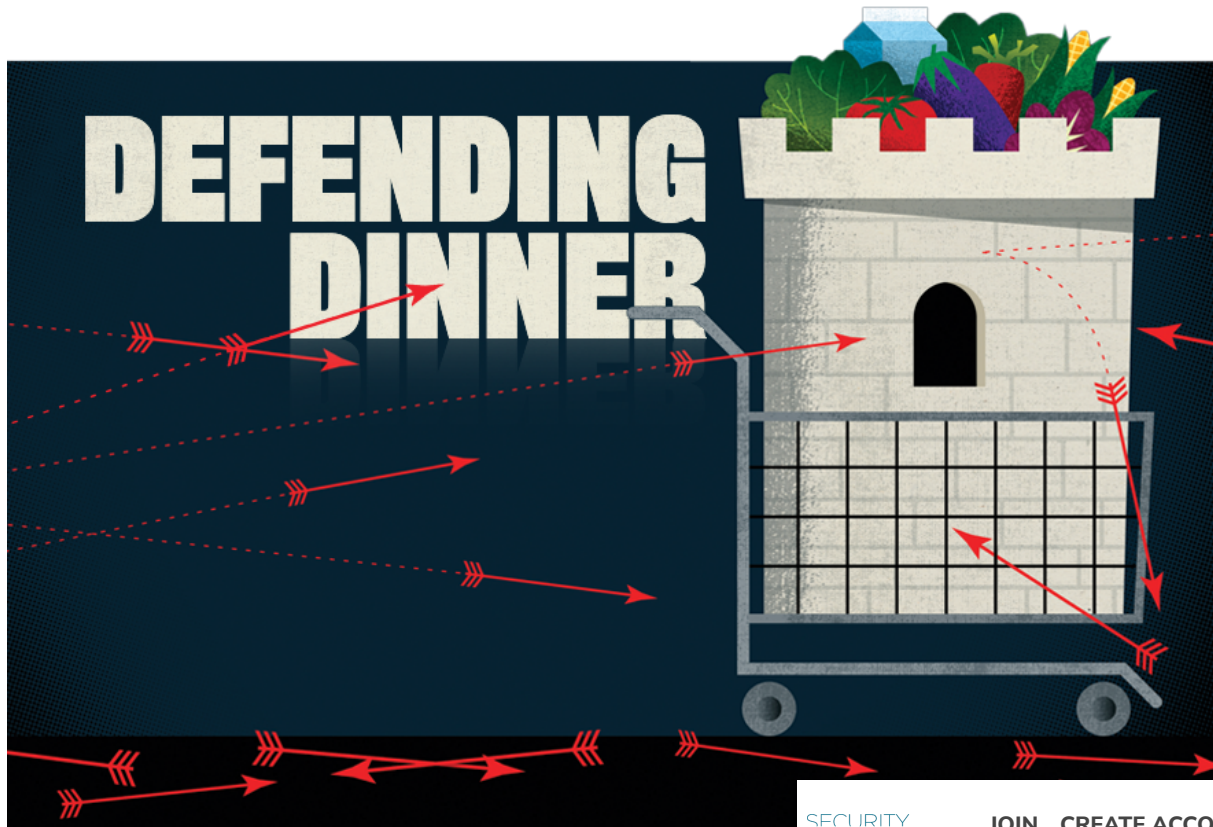




Protect your organization  
from cyber threats

Get your e-book

Genetec™



SECURITY  
MANAGEMENT  
A PUBLICATION OF ASIS INTERNATIONAL

JOIN CREATE ACCOUNT Q



Illustration by Michael Austin

FOOD AND AGRICULTURE RISK MANAGEMENT INSIDER THREAT

## Food Defense and the Insider Threat

By James T. Summers and Frank Pisciotta | 01 January 2020 |

Print Issue: January 2020

It was a story of strawberries, needles, and spite, and it launched a nationwide scare. In 2018, the Queensland police arrested a former strawberry farm supervisor for spiking supermarket strawberries with sewing needles, a crime that terrified consumers and crippled Australia's strawberry industry.

Prosecutors said the offender was motivated by "spite or revenge" over a

workplace grievance, and that her DNA was found on a needle recovered from a strawberry in Victoria. The episode led to more than 230 copycat incidents. That targeted attack on one company impacted an entire

industry, including six strawberry brands, and several supermarket chains stopped selling the fruit in response to the scare.

**[New] Newsletter**



## Subscribe to SM7

Find out your top seven security news stories, delivered to your inbox weekly, and powered by ASIS International.

[SUBSCRIBE NOW](#)

Food defense is the effort to protect food from acts of adulteration where there is an intent to cause harm to consumers. In the United States, the Food Safety Modernization Act Final Rule for Mitigate the Risk of Intentional Adulteration (IA) U.S. Food and Drug Administration (FDA) in May 2016, establishes a compliance framework for regulated facilities.

Like counterterrorism laws for many industries, the IA Rule requires regulated facilities to prepare a security plan—in this case, a food defense plan—and conduct a vulnerability assessment to identify significant vulnerabilities that, if exploited, might cause wide-scale harm to public health, according to the FDA. A failure to properly recognize the broader scope of insider threats could pose a significant risk to an organization's brand. A single incident could prove harmful enough to put a company out of business.

The FDA requires that regulated facilities consider insider threats, stating that the radicalized insider is the highest risk. The particular focus of the IA Rule, however, is the “wide-scale public health impact” caused by

rate, however, is the wide-scale public health impact caused by terrorism versus other threat scenarios such as acts of sabotage or adulteration committed by disgruntled employees, consumers, or competitors.

**The evidence points to a much higher likelihood of insider attacks against the food supply for reasons other than terrorism.**

Given the number of recent incidents, however, the evidence points to a much higher likelihood of insider attacks against the food supply for reasons other than terrorism, meaning it is critical for every organization to improve its ability to identify an inside attacker. The challenge for the industry is that information on how to properly identify insider threats is generally inadequate.

It is helpful in the context of identifying profiles for the food and beverage industry to utilize the offender classification scheme for workplace violence offenders. An insider threat detection program uses site-specific profiles, tripwires, and educated employees to move from a reactive to a proactive posture.

SECURITY  
MANAGEMENT  
A PUBLICATION OF ASIS INTERNATIONAL

JOIN CREATE ACCOUNT



However, this is far from simple.

Most organizations find it easy to believe that “nothing will ever happen here.” Employees tend to be reluctant to report coworkers, and this unwillingness can be magnified in workplaces with organized labor. Additionally, privacy concerns often prevent important information from being shared appropriately. For example, if a company knows that an employee has domestic violence concerns but HR fails to share that information with the security department in the interest of privacy, the company is missing an opportunity to proactively address risk. If informed, the security team could assist in detecting a trespass or provide additional protective services to the employee or the workplace.

## Offender Profiles

There are five main types of workplace violence offenders, and each could apply to the food and beverage industry.

**Type I.** This offender has no legitimate relationship to the business or its employees; rather the violence is incidental to another crime, such as robbery, shoplifting, or trespassing. In the food and beverage industry, this usually correlates the least to acts of intentional product adulteration. Potential motivations in this type—which have been seen in recent incidents—include social media fame-seeking, copycat attacks, extortion, or economic motives.

**Type II.** This offender has a legitimate relationship with the business—as a customer, client, patient, student, or inmate, for example—and becomes violent while being served by the business. Within the food and beverage industry, truck drivers represent a viable threat to an act of intentional adulteration, especially if they are made to wait for loading or unloading, costing the driver time and money.



**Type III.** This could be a current or past employee who attacks or threatens other employees in the workplace. This could spill over into product contamination if an employee attempts to adulterate a product to create problems for a coworker or supervisor, if the employee is irate over

compensation, or if the employee seeks revenge against the company by harming the brand.

**Type IV.** This offender may or may not have a relationship with the business, but he or she has a personal or perceived relationship with an employee. Domestic violence falls into this category. An employee's estranged spouse who is employed at the same site, for example, could attempt to adulterate product to create problems for the estranged spouse or endanger his or her livelihood.

**Type V.** This type of violence is directed at an organization, its people, or its property for ideological, religious, or political reasons. The violence is perpetrated by extremists or value-driven groups who feel justified by their beliefs. This is the type of offender that is the focus of the FDA's Intentional Adulteration Rule, but there is no known incident history in the United States for this offender category that resulted in a wide-scale public health impact. According to the FDA, acts of terrorism affecting the food and beverage industry—while not likely to occur—could cause illness, death, or economic disruption of the food supply absent mitigation strategies.

The profile of an insider threat in the food and beverage industry needs to be expanded far beyond the radicalized terrorist using the model above.

Formalized insider threat detection programs are government and IT space, but given the regulator experience from recent serious security incidents, this program is a critical consideration for the food and beverage industry.

SECURITY  
MANAGEMENT  
A PUBLICATION OF ASB INTERNATIONAL

JOIN CREATE ACCOUNT



## Insiders at Work

A supermarket in Grand Rapids, Michigan, recalled 1,700 pounds of ground beef after 111 people fell ill with nicotine poisoning. An employee at the store had mixed insecticide into the meat in an attempt to get his supervisor into trouble. Fortunately, although the amount of insecticide in a quarter-

pound burger made from the tainted meat could have been lethal, nobody died or suffered long-term health effects. This case demonstrates how an interpersonal conflict at work could be the motivation to contaminate product. The offender was sentenced to nine years in prison.

## ASIS Webinars

### Reach New Heights



*Security Management's* range of dynamic webinars, powered by ASIS International, can help you jumpstart your professional development.

REGISTER FOR FREE

In June 2016 in Minnesota, a woman was sentenced to 90 days in jail after being convicted of two felony counts of causing damage to property in the first degree. She was also required to pay \$200,000 in restitution. The company discovered sand and black soil in its chicken products. Video recordings were used to identify her as a person of interest in the case, and law enforcement was able to get a confession. After the incident, system improvements in the facility included adding video surveillance, requiring employee training that explains it is a crime to contaminate product, and the establishment of a partnership with HR to ob at-risk team members.

SECURITY  
MANAGEMENT  
A PUBLICATION OF ASIS INTERNATIONAL

JOIN CREATE ACCOUNT





---

In 2014, approximately 2,800 people in Japan were sickened by consuming frozen foods that had been contaminated with pesticide during production by a contracted worker who was apparently disgruntled about his low salary. Had the contract worker said anything about his displeasure with the pay rate? If so, did anyone question why a potentially disgruntled employee should be in such a sensitive position?

## Threat Detection

With the right set of insider threat detection measures, it is possible to reduce the likelihood of a successful insider attack like the ones outlined above. The Carnegie Mellon University Software Engineering Institute published its ***Common Sense Guide to Mitigating Insider Threats, Sixth Edition***, in December 2018. The document features helpful guidance that can be used to stand up an insider threat detection program, but this is an effort that can take a lot of time and resources.

In the meantime, set some early priorities to address the low-hanging fruit of insider threat detection.

**Personnel screening.** Food and beverage organizations generally know where their points of vulnerability and critical assets are. It is important to be cognizant of who has access to those critical assets or vulnerable processes.

Know who is working on site—whether employees or contractors—and encourage everyone to report concerns to management. Verify that potential employees have undergone a thorough background investigation, which should include criminal background and credit checks, where allowable under state and federal laws.

Encourage all employees to report suspicious behavior to management or through alternate channels with enough details to allow for an investigation. Employers must investigate and document all reports of suspicious or disruptive behavior. Enforce policies and procedures consistently for all employees. Consider an employee assistance program (EAP) that will help employees deal with personal issues confidentially.

**Address grievances.** When coupled with specific and precipitating events, specific insider personalities can create explosive results in terms of

workplace disruption or—in the case of food and beverages—an act of intentional adulteration.

The thread of grievance ran through many of the recent serious adulteration incidents perpetrated by insiders. Start by identifying common causes or signs that might represent the embers of a grievance (for example, peer-to-peer or subordinate-to-supervisor disagreements, confrontations with management, disputes or arguments, being passed over for promotion, demotion, intimate partner breakup, poor performance reviews, or workplace embarrassment).



**Security awareness training requires persistence, creativity, and multimedia messaging.**

Train supervisors and management teams to recognize tripwires. People who are observed overreacting to minor events, from serious adverse reactions to major events, such as a workplace. Other tripwires that can be included in employee training for insider threat detection might include changes to a person's baseline behavior. Coworkers are likely to notice such a change, and this should be cause for concern—especially when coupled with a precipitating event in the employee's life such as a divorce or a death in the family.

All of this requires a response in real time, so develop plans well in advance and train on them regularly.

## **Response**

Enhance monitoring for employees with impending or ongoing personnel or work performance issues, in accordance with organizational policy and laws. Enable additional auditing and monitoring controls outlined in policies and procedures



policies and procedures.

Be mindful of employees who self-report for conflict resolution or a change based on an adverse work environment. If an employee is looking for help

with conflict with a coworker, companies may wish to step up any observations of the employees involved in the conflict.

Increase random supervisory checks of workers involved in grievance events. Move employees involved in a grievance out of highly sensitive procedures where those employees may be working in isolation.

Increase active monitoring of people entering the facility and accessing the good manufacturing practice (GMP) areas of the plant.

### ASIS Certificate



## Introducing the New Executive Protection Certificate

Designed to give you the foundational knowledge and skills you need to become a more dynamic security professional, including EP specific threat and risk assessment, protection, advance planning and more.

SECURITY  
MANAGEMENT  
A PUBLICATION OF ASIS INTERNATIONAL

JOIN CREATE ACCOUNT



SIGN UP TODAY

Like active shooter incidents, intentional adulteration incidents seem to spawn copycat incidents, especially immediately after media coverage. Many copycats are social media fame-seekers who adulterate a product and post the photo or video online to get the “likes” and the publicity. Increasing monitoring for adulteration and grievances after a publicized incident is essential. The job of the food defense professional is not getting easier.

Ensure that the appropriate background checks are conducted in an

attempt to verify potential relations between replacement workers and striking workers, which could introduce an insider threat element in the event of a labor dispute that uses replacement workers.

Had these measures been in place, one U.S. production company could have screened out a man with a personal grudge against his employer. This individual filmed himself contaminating food on a production line and uploaded the video to the Internet as retaliation. While this incident caused no known illnesses, the employee intended to harm the company by making his video public on a popular website. The offender was arrested, convicted, and sentenced to 10 months in federal prison in 2019.

## Employee Education

The U.S. Department of Homeland Security’s “If You See Something, Say Something” campaign should be leveraged and even expanded if there is any chance of detecting an insider threat in the industry. Are companies properly defining irregularities that might be seen (such as changes in baseline behavior from a coworker), educating employees that some threats might be “heard,” and creating a climate for simple confidential reporting? Some programs expand “See Something, Say Something” to more of a “See Something, Hear Something, Say Something, Do Something” culture—a critical element of an insider threat management program.

SECURITY  
MANAGEMENT  
A PUBLICATION OF ASIS INTERNATIONAL

JOIN CREATE ACCOUNT



A good employee education effort can include new-hire training for food defense and specific training for people working at vulnerable points in the production process (both of which are mandated at FDA-regulated facilities under the IA Rule); periodic huddles or short presentations at the beginning of shifts to keep security and food defense top of mind for employees; and sharing the results of penetration or challenge tests intended to simulate breaches of security or food defense measures. Security awareness training requires persistence, creativity, and multimedia messaging.

## Conclusion

The food and beverage industry is under pressure to implement programs to mitigate the insider threat for intentional adulteration incidents with wide-scale public health impact. Incident history suggests that the profile

of likely offenders needs to be expanded, and the workplace violence offender profile offers an excellent starting point for the food and beverage industry.

Beyond official regulations, the ASIS International Food Defense and Agriculture Security Council provides an additional source of guidance about this risk, as do other open sources such as the Carnegie Mellon University insider threat guide mentioned previously.

Personnel surety is a critical strategy in protecting the food and beverage supply. Developing a focus on workplace grievances offers another opportunity to seize low-hanging fruit in identifying the potential for insider threats. Lastly, it is vital to educate managers, supervisors, and employees to be effective detection sensors in the battle to identify emerging insider threats that can result in product contamination, brand damage, and loss of jobs.

*James T. Summers is the director of security for North America at Kellogg Company and is the current Chair of the ASIS Food Defense and Agriculture Security Council.*

*Frank Pisciotta, CSC (Certified Security Consultant), is president of Business Protection Specialists, Inc., a nationwide independent security consulting firm focused on risk and regulatory compliance, development of global security programs, and security design services. He is also the Vice Chair on the ASIS Food Defense and Agriculture Security Council. He can be reached at [fp@securingpeople.com](mailto:fp@securingpeople.com).*

SECURITY  
MANAGEMENT  
A PUBLICATION OF ASIS INTERNATIONAL

JOIN CREATE ACCOUNT



# LATEST NEWS



## FCC Bans Some Chinese Telecommunications and Surveillance Equipment Sales

PHYSICAL AND OPERATIONAL SECURITY



## Diversity, Equity, and Inclusion: Why It Matters

MANAGING ORGANIZATIONS

SECURITY  
MANAGEMENT  
A PUBLICATION OF ASIS INTERNATIONAL

JOIN CREATE ACCOUNT



## Insurgency Threatens to Spill Across the Sahel, Ghanaian President Warns

NATIONAL SECURITY



## Recent Shootings Call into Question Efficacy of Red Flag Laws

RISK MANAGEMENT

INFRASTRUCTURE

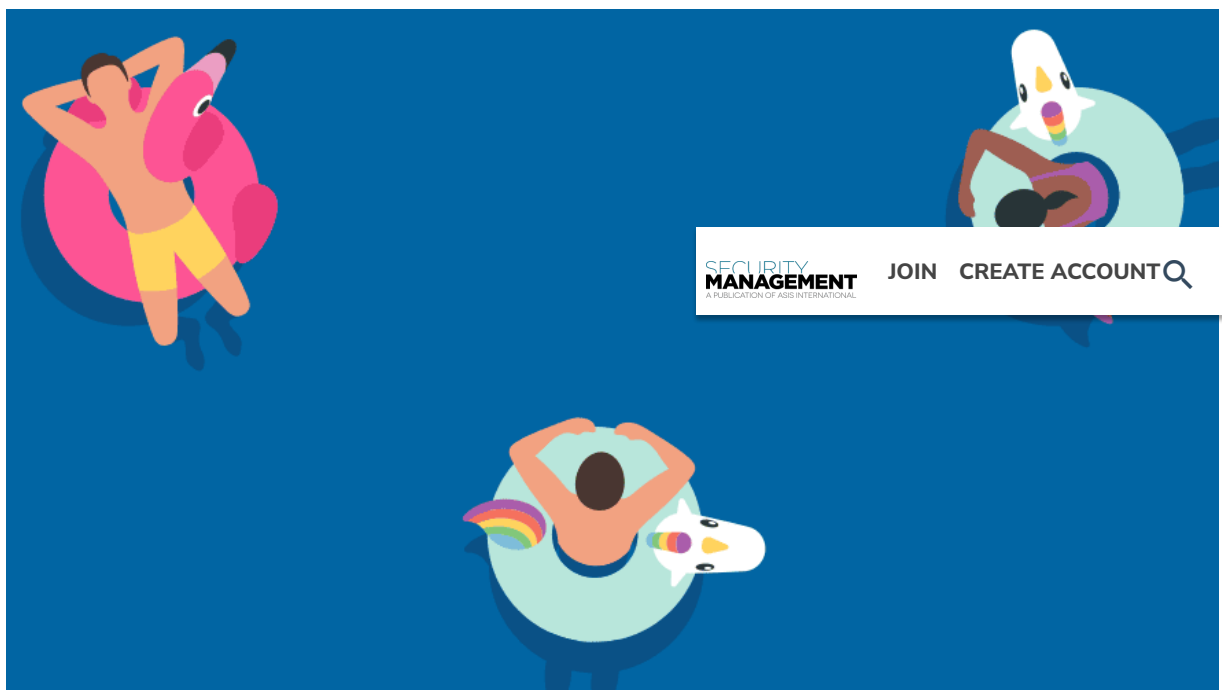
# ComNet Connects



AIRPORT


**comnet** Transmission Solutions for the Long Run

## TRENDING NEWS



**SECURITY MANAGEMENT**  
A PUBLICATION OF ASIS INTERNATIONAL

[JOIN](#) [CREATE ACCOUNT](#)



## Collateral Damage: Cartel Activity Spills Over into Tourist Resorts



Nearly Half of All U.S. Murders Went Unsolved in 2020



Recent Shootings Call into Question Efficacy of Red Flag Laws



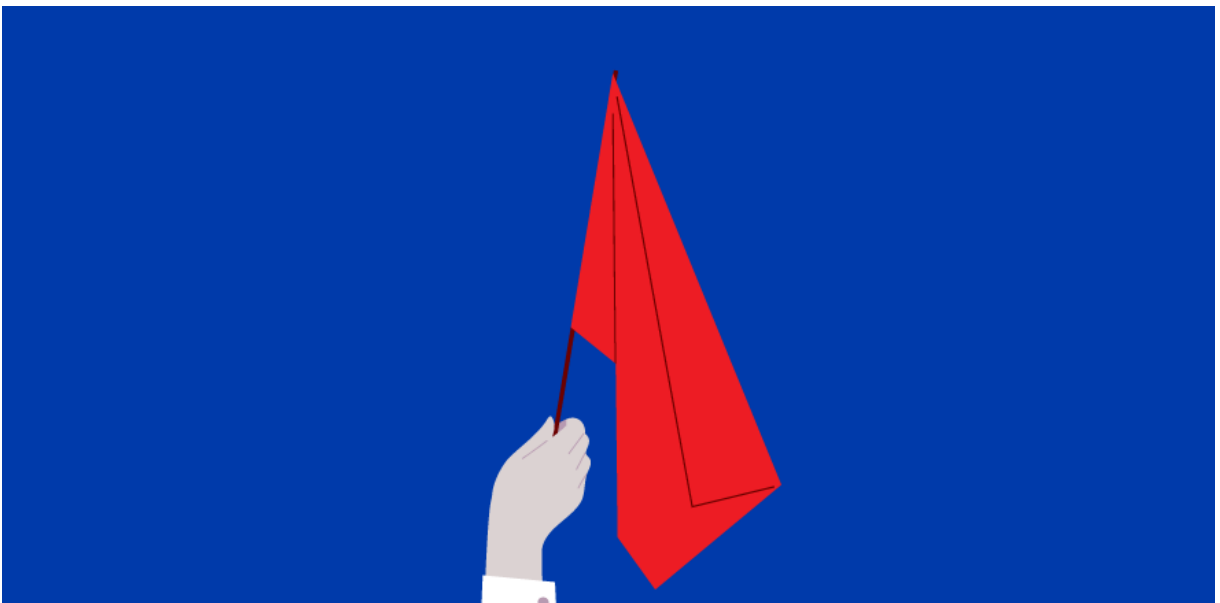
Your First 90 Days as a New Leader

SECURITY  
MANAGEMENT  
A PUBLICATION OF ASB INTERNATIONAL

[JOIN](#) [CREATE ACCOUNT](#)



# MORE FOR YOU





## Recent Shootings Call into Question Efficacy of Red Flag Laws

RISK MANAGEMENT



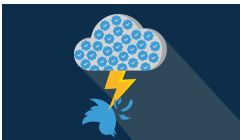
### Investigators Assess Whether LGBTQ Nightclub Attack Was Hate Crime

CRIME



### Healthcare NGO Partners for Risk Management Assistance

HEALTH CARE



### Twitter Verification Changes Unleash Deluge of Impersonations, Misinformation, and Reputation Risks

INFORMATION TECHNOLOGY AND  
TELECOMMUNICATIONS

SECURITY  
MANAGEMENT  
A PUBLICATION OF ASIS INTERNATIONAL

JOIN CREATE ACCOUNT 



# ASIS NEWS

Security Management is Going Digital

NEWS



Leadership Lessons from a Legend Series: What Don W. Walker, CPP Taught the Security Profession

NEWS

# ASIS

INTERNATIONAL



Featured NextGen Member Q&A: Pablo Nicolas Espinosa, APP, PSP

NEWS

SECURITY  
MANAGEMENT  
A PUBLICATION OF ASIS INTERNATIONAL

JOIN CREATE ACCOUNT



Congratulations to Our Newly Board-Certified Security Practitioners for October 2022

NEWS

**lobby**

Streamlining Visitors in a High-Security Environment

READ OUR CASE STUDY



