

AGRICULTURE AND FOOD SECTOR RISK ANALYSIS

*Randall R. Nason, PE, Vice President
C.H. Guernsey & Company*

*David Cid, President
David Cid Consulting, LLC*

INTRODUCTION

The importance of the food sector to our national security and economy was highlighted in the 2003 Homeland Security Presidential Directive 7 (HSPD7) which established a joint public and private sector partnership to develop security guidelines and standards for the various critical infrastructure sectors, including the food sector. The increased emphasis on food security was also validated with the passage of the Food Safety and Bioterrorism Act in 2002.

An essential first step in developing a food security program is to perform a **vulnerability analysis and risk assessment (VRA)**. A VRA is an important tool in identifying the risks, including homeland security concerns associated with a particular portion of the agriculture and food sector. Very briefly, the VRA identifies assets critical to the reliable and efficient business performance of the food-related organization and directs formulation of preventative measures designed to reduce the vulnerability of the critical assets to the identified threat.

A VRA can be thought of as three interrelated and complementary efforts.

The first and most essential component of the vulnerability analysis is the terrorism threat assessment. The terrorism threat assessment provides a fundamental indication of individuals and groups that have an interest in causing damage to organizational assets.

The VRA is an effective tool in guiding the development of a food organization's security program. The VRA will help:

- Prioritize implementation of preventative measures, reducing vulnerability, and therefore the risk to identified threats
- Direct the development of mitigating measures, reducing the magnitude of a potential loss

The second is a vulnerability analysis which identifies those physical components, processes, information, and staff that are essential to the reliable and efficient performance of business. Once these assets are identified, their level of exposure to the threat spectrum can be evaluated.

Third, the risk assessment takes the results of the threat assessment and vulnerability analysis and derives an indicator of the risk associated with a particular critical asset.

This package describes a general process for conducting a VRA, with a particular emphasis on terrorist-related or other intentional man-made events. Other types of events affect food-related systems, facilities, and business processes. These include weather-related events such as tornadoes, hurricanes, ice storms, and mud slides as well as man-made accidental incidents such as toxic chemical spills on nearby rail lines or highways. In many cases, food-related organizations have dealt with these types of incidents in the past and have some level of emergency restoration plan in place. However, potential terrorist-related incidents and other intentional man-made events are somewhat new to the food community. Therefore, this package provides the tools to allow the food community to evaluate their risk for this new category of events effectively and prudently. In addition, the general process described herein can also be applied to the weather and accidental events discussed above.

BASIC CONCEPTS

The concept of risk management for a food-related organization is based on six fundamental premises.

SIX PREMISES

- Food organizations possess a variety of **assets**. Certain assets are considered critical assets and are vital to the efficient and reliable functioning of the business.
- Each of these critical assets is **vulnerable** to being damaged or destroyed by a variety of means, so that the function it provides is no longer available. However, proactive, preventative measures such as lighting, electronic entry control, and CCTV monitoring can reduce the vulnerability of the asset.
- Groups or individuals pose a **threat** to the critical assets. The degree of the threat will vary, but it does exist at some level. The goal of the threat is to cause loss to the food organization (e.g., loss of life, personal injury, lost revenue, repair costs, lost data, damaged reputation).
- The **likelihood** of a critical asset's damage or destruction is a function of the threat combined with the vulnerability or attractiveness of the asset.
- For each critical asset, there are results or **consequences** to the food business if the asset is damaged or destroyed. Mitigating measures can and should be developed to reduce the consequences of these events.
- **Risk** is a measure of an organization's exposure to loss and is a function of the likelihood of the loss combined with the potential magnitude of that loss.

These six premises contained six key terms. It is important to understand these terms within the context of the food industry.

Asset: An asset is anything a food organization owns or uses in the conduct of its business. Assets range from “hard” assets such as silos, mills, ovens, storage elevators, feed lots, warehouse facilities, and information technology (IT) infrastructure to “softer” items such as trained staff, brand name recognition, and a strong community reputation. A **critical asset** is any plant, facility, research laboratory, component, information system, data file, staff position, or support function essential for the food organization to conduct its business.

Assets include anything or anyone the food organization relies upon in the conduct of its business

Critical assets are those assets that are *absolutely essential* to the conduct of the food organization’s business

Vulnerability: Vulnerability is any aspect of an asset that can be exploited to bring about an undesired, detrimental outcome. Examples include an unlocked door to the organization’s headquarters facility, a transport truck with keys left inside, unscreened visitors, or a substation transformer that is easily visible from the adjacent highway. Each of these represents an opportunity for an individual or group with malevolent intentions to cause damage and loss to a food organization’s operation.

Vulnerabilities include any aspect of a food organization’s assets that could be exploited to bring about a detrimental, undesired result.

Threat: Threat can be defined as the potential for harm. Using this definition, weather can properly be considered a threat to the system. However, the primary threat emphasis in this paper is on terrorism or other intentional, man-made actions that can result in an undesired, detrimental result.

Threat is the potential for harm from malevolent man-made events.

Likelihood: The likelihood, or qualitative probability, of an event is a composite term. Likelihood depends on the specific threat that might be directed at a critical asset and the nature or attractiveness of the asset vulnerability.

Likelihood deals qualitatively with the probability of an undesired event. It is a function of the magnitude of the threat and the attractiveness of the critical asset to the goals of the perpetrators.

Consequences: Consequences are the direct and indirect results of an undesired event which may include damage to a “hard” asset (such as a silo, sifter, production equipment, or on-site electrical transformer) and “softer” assets (such as a tarnished reputation among consumers). The magnitude of the consequences will vary depending on the event. For example, a passerby

shooting the on-site power supply equipment may represent a different type and magnitude of loss than the headquarters facility being vandalized after hours due to an unlocked door.

Consequences are the direct and indirect results of an undesired event.

Examples of loss include:

- Shutdown of process due to loss of essential utility support such as electrical power or water supply
- Interruption in the supply of feed material to the production process as a result of damage to the conveyor system
- Inability to process and distribute bills to upstream customers due to computer disruption/downtime caused by physical damage or a virus

Risk: Risk is a composite measure of an organization's exposure to loss. While risk can be defined in a number of ways, a simple working definition is the product of the likelihood of an undesired event and the magnitude or severity of the consequences associated with that event. With this definition, for a given outcome the risk increases as the likelihood of the event increases. Similarly, for a given likelihood, the risk increases as the severity of the consequences increase.

Risk is a composite measure of a food organization's exposure to loss and is a function of the likelihood of an event and the projected consequences of that event.

THE VRA PROCESS

WHAT ARE THE STEPS TO COMPLETING A VRA?

The VRA process can be organized into five steps as shown in Figure 1. Very briefly, these steps are:

Step 1: Terrorism Threat Assessment. A vulnerability analysis is performed based on the assumption that there is a threat to the food organization's assets.

Step 2: Vulnerability Analysis. The fundamental purpose of a vulnerability analysis is the identification of those food organization assets essential to efficient and reliable business performance. Critical assets can range from physical components (e.g., production facilities, substation transformers, headquarters facility, and information technology infrastructure) to soft assets (e.g., work processes, reputation among consumers). Assessing the threat to and vulnerability of a specific asset leads to an indication of the likelihood of an undesired event involving that asset.

Step 3: Estimation of Consequences. Exploitation of asset vulnerabilities produces undesired, detrimental results. Depending on the specifics of the incident, the consequences can range from minor damage resulting from vandalism and graffiti to incidents with significant, long-term impacts to the food organization's revenue, profitability, and consumer reputation.

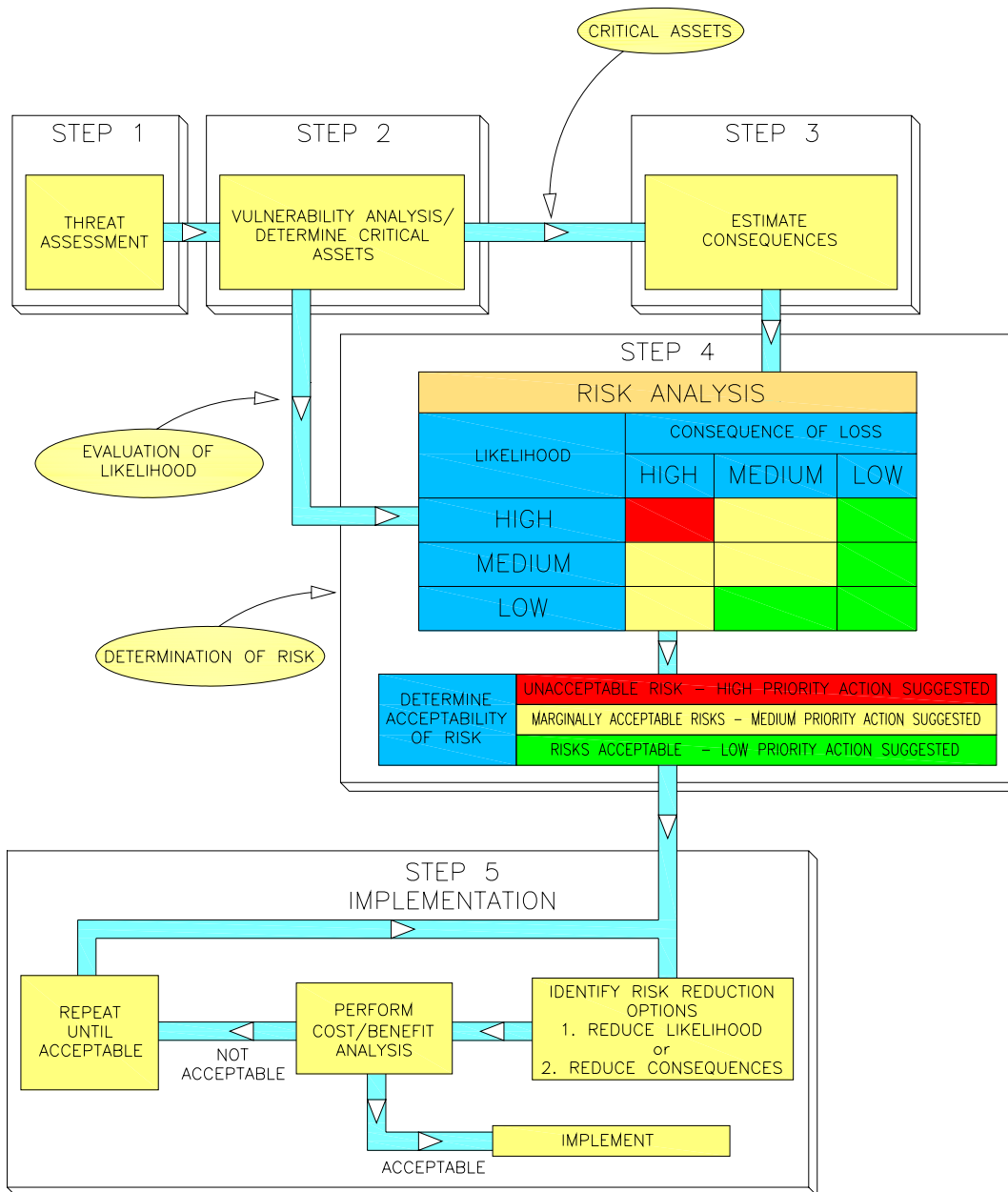
Step 4: Determination of Risk. Risk is the qualitative product of the likelihood of an event and the consequences associated with that event and represents the organization's level of exposure to loss.

Step 5: Implementation. The goal is to minimize an organization's risk from both natural and man-made events. The risk assessment provides an indication of risk to the critical assets. Risk can be lowered by:

- Preventive measures that reduce the vulnerability of the asset
- Mitigating measures that reduce the consequences associated with loss or damage of the asset

Implementing either preventive or mitigating measures normally requires careful thought and planning to ensure optimum effectiveness.

The threat assessment discussed herein is primarily directed at terrorism threats. Natural "threats" (primarily weather) are well understood by the food community and are normally preceded by some advance warning. Whereas storm planning relies heavily on historical storm patterns, planning for man-made threats represents an extension of the storm planning process – with two significant differences. First, the consequences from a man-made event may be more severe than for a weather-related event. Second, there will likely be no advance warning of a man-made event.



COMPLETING THE VRA

The following sections address the five steps of the VRA process, starting with the terrorism threat assessment. The terrorism threat assessment provides the basis for identifying vulnerabilities associated with critical assets. Each subsequent step in the VRA process builds upon the results in previous steps.

STEP 1: TERRORISM THREAT ASSESSMENT

Threat can be defined as the potential for harm. In this context, threat is defined as the potential for harm from intentional man-made events. A threat assessment attempts to measure one aspect of the likelihood of harm. The higher the threat level, the greater the likelihood that the harmful, undesired event will occur. To reduce risk in an efficient way, we must recognize that some threats are more likely to occur than others. A terrorism threat assessment attempts to provide the first step in answering the question, “What is the likelihood that our assets will be attacked in a malevolent, intentional manner?”

A **threat assessment** is a judgment, based on validated information, of the character, nature, and probability of a threat

Threat assessment is a critical phase of the VRA process, since failure to properly identify threats can lead to failure to reduce the risks they present. As stated earlier, this guide primarily addresses the development of a terrorism threat assessment although the process can in general address the man-made threats, such as those from disgruntled employees and criminals.

Threat Assessment Process

1. Plan data collection activities by identifying federal, state and local law-enforcement contacts in your area of concern. Determine which databases and other sources you will query
2. Collect data
3. Validate data by discussing all positive findings with law-enforcement authorities
4. Assign positive findings to one of three metrics of threat: Presence, Capability, Interest-Intention
5. Assess “Other Considerations in Determining Threat Levels” (See suggested list, in this Guide)
6. Measure your organization's threat level
7. Incorporate your threat assessment into the overall Vulnerability Analysis

BACKGROUND

Law-enforcement and intelligence agencies conduct the most accurate and sophisticated terrorism threat assessments. The Federal Bureau of Investigation (FBI), the United States Secret Service, and other law-enforcement organizations prepare local, regional, and national assessments of the terrorism threat in the United States. The assessments are either considered classified national security information or “Law Enforcement Sensitive” and are therefore not available to the public. However, these agencies are the preeminent authorities on terrorism and should be contacted for whatever information they are able to share. Eliciting information from the FBI and other law-enforcement entities is discussed later under “Collecting Data”

Threat assessments, though based on empirical data, are in fact heavily dependent on the role of judgment. Within and between law-enforcement and intelligence agencies there may be conflicting views on the nature and severity of the threat. Even with these limitations and uncertainties, the threat assessment remains a valuable security and planning tool.

TERRORISM DEFINED

Terrorists are individuals or groups that engage in criminal activity in support of a political or social agenda. Unlike the traditional criminal, the terrorist is motivated by ideology and deeply held beliefs. This makes the terrorist a more daunting adversary.

Terrorism is “the unlawful use of force or violence against persons or property to coerce a government, civilian population or any segment thereof, in furtherance of political or social objectives.” (28 CFR, Part 0.85)

Defining the Threat

Since past behavior is a factor in the prediction of future behavior, a review of acts of terrorism against the food industry is helpful. Historically, the terrorist threat to the food industry has come from environmental extremists who oppose genetically altered crops. They have attacked research facilities, experimental crop sites, and the offices of companies who engage in this type of activity. Because of the critical nature of a reliable and safe food supply, and the effect on our everyday life that contamination or disruption would have, other terrorist groups, particularly those affiliated with Al Qaeda, should be considered in the threat assessment as well. These attacks would likely be directed at critical hubs in the product cycle such as suppliers, manufacturing facilities, transportation assets, and processing plants, among others. Unlike the natural disaster, the thinking adversary would attack the food cycle at its most critical and vulnerable points. Therefore, countermeasures must be driven by an analysis from the standpoint of the adversary, answering the question: “If my goal was to disrupt the food cycle with maximum effect, when, where and how would I do so?”

Additionally, since Al Qaeda has recruited professionals from all walks of life, an underlying assumption of this analysis must be that the attacker may be well informed and have an understanding of the product cycle and its vulnerabilities.

Any group or individual may, at any time, commit an act of terrorism. Therefore, we must go beyond the examination of historical events. We must also examine the empirical data relevant to our particular community and region to conduct a timely, reality-based threat assessment. The local and regional threat environment are the most relevant to the development of security measures, since the most probable threat is likely to come from terrorist groups or individuals in your area of concern. *

* Define your area of concern as your locality, state or region, depending on the geographic distribution of your assets.

Terrorism: A REVIEW OF PAST ACTS

December 3, 2002 - Northwestern Pennsylvania

The Earth Liberation Front (ELF) claimed credit via communiqué for destroying a test/demonstration crop of BT Genetically Modified Organism (GMO) corn.

December 3, 2002 - Northwestern Pennsylvania

The Earth Liberation Front (ELF) claimed credit via communiqué for destroying a test/demonstration crop of Roundup-Ready Genetically Modified Organism (GMO) corn.

January 26, 2002 - St. Paul, Minnesota

The Earth Liberation Front (ELF) claimed credit for setting a fire at 4:00 a.m. at a University of Minnesota research laboratory and construction site of the Microbial and Plant Genomics Research Center. Specifically, the fire damaged several pieces of construction equipment, a construction trailer, and several research labs in an adjoining building. The communiqué claimed the fire was set to protest school-sponsored research on genetically modified crops. Initial damage estimates were a minimum of \$250,000, with expectations that actual damages would be much higher—possibly reaching \$1 million.

Early January 2002 - Fairfield, Maine

Construction equipment at the new Jackson Labs biotech facility was monkey wrenched by the Animal Liberation Front (ALF) and the Earth Liberation Front (ELF).

November 5, 2001 - Houghton, Michigan

Bombs were successfully disarmed at two buildings at Michigan Technological University. Specifically, the devices were discovered at 3:35 a.m. by campus security officers at the Ubald J. Noblet Forestry Building and the U.S. Forest Service Engineering Laboratory. Genetic research is conducted in both buildings. The university previously received threats from the Earth Liberation Front (ELF); the latest occurred in April 2001. The bombs consisted of five-gallon buckets filled with a liquid and wired to ignition devices.

August 21, 2001 - Woodbury, New York

The Earth Liberation Front (ELF) claimed credit for vandalizing the Cold Spring Harbor laboratory's new Woodbury facility, located in Nassau County, Long Island, where scientists conduct cancer research. Damages amounted to approximately \$20,000 and consisted of breaking a window, spray-painting graffiti, and breaking a thermostat that controls the building's air conditioning. In their claim and in their graffiti, ELF made references to "biotech kills" and specifically to genetically modified corn. The 12-acre Woodbury facility, however, is involved in cancer research and has no involvement in genetically altering plants.

June 10, 2001 - Moscow, Idaho

The Earth Liberation Front (ELF), Night Action Kids cell, claimed responsibility for sabotaging the new \$13 million agricultural biotechnology building at the University of Idaho in opposition to genetic engineering. The group claimed that this attack was the second to be staged at the building. During the June 10 incident, ELF claimed that it removed survey stakes and spray-painted graffiti on the building's exterior. Damages totaled close to \$500; however, damages from the first spray-paint attack by ELF, on March 11, 2001, totaled more than \$4,000.

Terrorism: A REVIEW OF PAST ACTS (continued)

May 21, 2001 - Clatskanie, Oregon

The Earth Liberation Front (ELF) used incendiary devices to destroy two buildings and a number of vehicles—including pickup and flatbed trucks, all-terrain vehicles, and a semi trailer—at Jefferson Poplar Farm. Incendiary devices that failed to ignite were also found in the building housing the farm's offices. This attack occurred at approximately the same time as a three-alarm fire destroyed the University of Washington's Center for Urban Horticulture, located approximately 100 miles to the north. The previous owners of Jefferson Poplar Farm were affiliated with a University of Washington-based group called Popular Molecular Genetics Cooperative. Damages at Jefferson Poplar Farm's facility totaled at least \$500,000. ELF graffiti was discovered at the site, and ELF claimed credit via a communiqué.

May 16, 2001 - Brentwood, California

Antigenetic engineering activists entered the DNA Plant Technology research facility and destroyed strawberry, tomato, and onion plants. Specifically, a one-acre field of strawberries was uprooted and the plants placed in bleach-filled plastic bags to prevent replanting. One-quarter acre of fruiting tomato plants in a greenhouse were also destroyed, as well as one-half acre of mature onion plants.

March 11, 2001 - Moscow, Idaho

The Earth Liberation Front (ELF) spray-painted graffiti on the new \$13 million agricultural biotechnology building at the University of Idaho, resulting in over \$4,000 in damages. This antigenetic engineering attack was claimed via a communiqué issued by ELF in connection with their June 10, 2001, attack at that same university.

February 20, 2001 - Visalia, California

Earth Liberation Front (ELF) claimed that it burned a research cotton gin at Delta and Pine Land Company. The action was in opposition to the genetic engineering of plants to produce sterile seeds. Specifically, the ELF communiqué expressed concern for what it called "Terminator Technology" and claimed, "Engineering a suicide sequence into the plant world is the most dangerous new technology since nuclear power and needs to be stopped." Damages were estimated at \$700,000.

October 5, 2000 - Kauai, Hawaii

The activist group Menehune destroyed experimental papaya, pineapple, and orchids at the University of Hawaii/United States Department of Agriculture (USDA) Research Center.

September 5, 2000 - Kauai, Hawaii

The activist group Menehune destroyed a test plot of genetically modified corn at Novartis Research Center.

August 10, 2000 - Davis, California

Reclaim the Seeds destroyed genetically engineered corn at the University of California. The group videotaped masked activists using a long-bladed scythe to cut the corn. Eighty percent of the corn was destroyed, with only the outer rim left standing to protect the attackers.

July 31, 2000 - Dusty, Washington

Five acres of genetically altered canola were destroyed at Monsanto facility by the Dusty Desperados.

July 19, 2000 - Rhinelander, Wisconsin

Over 500 trees/saplings were destroyed and 10 vehicles defaced to protest genetic engineering at the U.S. Forest Service, Central Research Station Forest Biotechnology Laboratory. The destroyed crops were valued at \$750,000 and the damages to the truck were \$20,000 (Earth Liberation Front [ELF]).

July 13, 2000 - Cold Spring Harbor, New York

Several acres of corn, as well as two years of genetic experiments, destroyed at Cold Spring Harbor laboratory (Earth Liberation Front [ELF]).

June 14, 2000 - Davis, California

Members of Reclaim the Seeds breached the security system of the Monsanto R & D unit at the firm's Calgene Campus and cut into and entered the greenhouses. An alarm caused the activists to leave before they were able to damage equipment and genetically altered crops.

June 4, 2000 - Canby, Oregon

Experimental plots of grass at Pure-Seed Testing facility were destroyed with \$300,000–\$500,000 in damages (Anarchist Golfing Association).

May 23 and 24, 2000 - Woodland, California

Over two evenings, a group calling itself Future Farmers of America destroyed genetically altered crops in greenhouses at Seminis Vegetable Seeds Research Center.

Measuring the Threat

Terrorism threat assessments should address three metrics:

Terrorism: A REVIEW OF PAST ACTS (continued)

May 21, 2000 - Albany, California

Members of Reclaim the Seeds were thwarted by security as they attempted to break into the U.S. Department of Agriculture (USDA), Agricultural Research Service, Western Regional Research Center.

May 10, 2000 - Manoa, Kauai, Hawaii

A group called Menehune destroyed fruits, including papayas and pineapples, and flowers, such as anthuriums and dendrobium orchids, at the U.S. Department of Agriculture (USDA), Agricultural Research Service.

May 9, 2000 - Kekaha, Kauai, Hawaii

Menehune destroyed one test plot of corn at the Novartis Research & Parent Seed Center and invalidated experiments by deliberately mixing pollens from test plots of corn.

April 8, 2000 - Sonoma County, California

Grape plant starts at a Vinifera, Inc. research plot were hacked and cut down by a group calling itself Petaluma Pruners.

April 1, 2000 - St. Paul, Minnesota

A group calling itself Genetic Jokers trashed the U.S. Forest Service facility at the University of Minnesota. Damages included etched windows, glued locks, defaced walls, slashed tires, and six damaged vehicles. Total damages were estimated at approximately \$20,000.

February 9, 2000 - St. Paul, Minnesota

Earth Liberation Front (ELF) broke into Green Hall at the University of Minnesota, targeting two professors' work on transgenic oats. All the oats were destroyed, the lab was spray-painted, and the locks were glued.

January 20, 2000 - Watsonville, California

A field of genetically modified strawberries at Plant Sciences, Inc., was destroyed by Fregaria Freedom Farmers.

January 11, 2000 - Albany, California

Reclaim the Seeds raided the Western Regional Research Center at the University of California's Plant Gene Expression Center, destroying one-half the crop of transgenic wheat and ruining the experiment.

Presence. Is a terrorist group – or an individual sympathetic to the group's agenda – located in your area of concern?

Capability. Does the group/individual have the ability to attack the food infrastructure?

Intent. Does the group/individual have the interest or intent to attack the food infrastructure?

These metrics are measured by inference. The most effective threat assessments are underpinned by sound empirical data. Generally, information will be from the intelligence community, law-enforcement agencies or public sources. Information from intelligence and law-enforcement sources is the most reliable. Other sources, such as media reports, may require validation. Validating is simply a matter of checking with more than one source to confirm the veracity of the information. The most reliable way to validate information you collect is to discuss it with law enforcement.

THE THREE METRICS

The three metrics – Presence, Capability, and Intent – are identified indirectly by the presence of certain indicators. Because they are identified indirectly, we must recognize that there is room for error. Threat assessment development is not a science; even the most skilled and experienced experts can be wrong.

It is critical to make judgments in the context of the overall security environment. For example:

- Isolated incidents do not have the same significance as a pattern of activity.
- Incidents in the distant past do not have the same significance as incidents that are more recent.
- Incidents involving vandalism do not have the same significance as incidents involving arson or destruction of property.
- Incidents involving high-visibility targets are more significant than those that do not.

The value of good judgment, common sense, and experience cannot be overstated in this process.

Presence

Although terrorists are capable of moving to a locality and mounting an attack, many acts of terrorism are carried out by locals. Proximity leads to access to the target and a personal investment in the community the individuals wish to affect by their actions. Clues to measuring Presence include:

- Local criminal activity by the group or its members
- Availability of literature supporting the group's agenda
- Public demonstrations by the group
- Media releases or other public statements by the group
- Acts of terrorism

Capability

Many radical groups engage in inflammatory rhetoric but lack the ability to carry out an actual attack. Clues to measuring Capability include:

- Viable, stable or growing membership
- Fund-raising or access to monies
- Active training
- Intelligence gathering or information-gathering by the group
- Knowledge of system vulnerabilities
- Access to system facilities
- Access to weapons or explosives
- Previous destructive actions

Intent

Intent is the least tangible metric, representing thinking and motivations. Like the other metrics, it is measured indirectly. Clues to measuring Intent include:

- Ongoing planning and preparation for an act of terrorism
- History of violence against food organizations or other components of the food infrastructure
- History of anti-government rhetoric
- Association with anti-government or terrorist groups
- Violent ideology
- Acts of terrorism

DETERMINING THREAT LEVEL

Using the three metrics, it is possible to rank the threat in your area of concern.

METRIC(S)	RANK THE THREAT AS...
None; no industry-specific alert <i>If there is no indication of Presence, and there is no industry-specific alert, no further analysis is required. Rate your terrorism threat level as "Low"</i>	Low
Presence	Guarded
Presence + Capability	Elevated
Presence + Intent <i>Capability may be quickly acquired.</i>	High
Presence + Capability + Intent	Severe

In the current national security environment, there is no area where threat does not exist. The highest threat exists when Presence, Capability, and Intent intersect. Absent any indication of Presence, Capability, or Intent, the threat from terrorism should be considered Low. An exception to this would be a national threat warning indicating the targeting of the food infrastructure. This would support the elevation of the threat level by one or more steps, depending on the details of the warning.

OTHER CONSIDERATIONS IN DETERMINING THREAT LEVELS

- If your facilities have been targeted or attacked in the past, elevate your threat level one step. For example, if your threat level is Guarded based on the presence of a radical group in your area, and your facility has been targeted or attacked in the past, raise your threat level to Elevated.

- If your organization or customers are engaged in sensitive or high-profile activities known to be of interest to terrorists, elevate your threat level one step. Examples of such activities could include production or testing of genetically altered plants.

CHARACTERIZING THE ADVERSARY

The most effective attack against a facility would be carried out by an individual with access and knowledge of the system’s vulnerabilities. The following chart characterizes adversaries by access and knowledge.

ACCESS →	<p>Uninformed Insider</p> <ul style="list-style-type: none"> • Limited or no knowledge • Unimpeded access to facility 	<p>Informed Insider</p> <ul style="list-style-type: none"> • Knowledge concerning facility operations and vulnerabilities • Unimpeded access to facility
	<p>Uninformed Outsider</p> <ul style="list-style-type: none"> • Limited or no knowledge • No access to facility 	<p>Informed Outsider</p> <ul style="list-style-type: none"> • Knowledge concerning facility operations and vulnerabilities • No access to facility
	KNOWLEDGE →	

CHARACTERIZING THE INFORMATION

As stated earlier, information should be assessed for accuracy and reliability. For example, information received from law-enforcement sources should be considered accurate and reliable. Open-source media reporting should be independently verified if possible.

Validating information can be a complex process. Advising authorities of any positive information from any other source is an excellent practice. It enables you to use the expertise of law enforcement to assist in validation, while ensuring that they are informed of your findings.

COLLECTING DATA

Law enforcement shares sensitive terrorism information on a very limited basis. Still, federal, state, and local authorities are the most authoritative sources in this area and should be contacted first.

- **Federal, state, and local law enforcement.** The FBI is the lead counterterrorism agency in the United States. Other federal agencies with counterterrorism responsibilities include the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF); the United States Marshals Service; and the United States Secret Service. Local agencies include sheriff's departments, and state investigative and enforcement departments, police departments, and state investigative and enforcement agencies such as the Department of Public Safety and the Highway Patrol.
- **Open-source media reporting.** Newspapers, both state and local, often cover the activities of radical groups, including public demonstrations and criminal acts.
- **Web-based resources.** Websites can offer both general and specific information concerning terrorism and terrorist groups. Please see the Additional Resources section of this Guide for a list of recommended websites.
- **Criminal complaints, indictments, and convictions.** Prosecutors are prohibited from discussing pending cases. However, there is no such prohibition for cases that have been adjudicated. In addition, under most circumstances, complaints and indictments are a matter of public record. All criminal convictions are a matter of public record.
- **Infragard.** Infragard is an FBI-sponsored collaboration with the private sector to enhance the security of critical components of the infrastructure. Each FBI field office has an Infragard representative who can provide details. **Every food organization association should be represented here.** This is also an excellent venue for interacting with the broader law-enforcement community, whose representatives are generally in attendance. Because members are vetted, discussions about the threat from terrorism are more open and frank than in other settings. Terrorism working groups have been established in some FBI field offices as well. Contact information for each field office may be found at www.fbi.gov or at www.infragard.net.
- **Department of Homeland Security Advisories and Bulletins.** The Homeland Security Advisory System is designed to target protective measures when information specific to a particular sector or geographic region is received. It combines threat information with vulnerability assessments and provides communications to public safety officials and the public.
- **Homeland Security Threat Advisories** contain actionable information about an incident involving – or a threat targeting – critical national networks, infrastructures or key assets. Advisories could, for example, relay newly developed procedures that, when implemented, would significantly improve security or protection. Advisories are targeted to federal, state, and local governments, private sector organizations, and international partners.
- **Homeland Security Information Bulletins** communicate information of interest to the nation's critical infrastructures that do not meet the timeliness, specificity, or significance thresholds of warning messages. Such information may include statistical reports, periodic summaries, and patches, common vulnerabilities, and configuration standards or tools. It also may include preliminary requests for information. Bulletins are targeted to federal, state, and local governments, private sector organizations and international partners.
- **The Color-coded Threat Level System** is a threat-based system used to communicate with public safety officials and the public at large so that protective measures can be implemented to reduce the likelihood or impact of an attack. Raising the threat condition has economic, physical, and psychological effects on the nation. Therefore, the Homeland

Security Advisory System can place specific geographic regions or industry sectors on a higher alert status than other regions or industries, based on specific threat information.

- **The Department of Homeland Security (DHS) Information Analysis and Infrastructure Protection (IAIP)** serves as a national critical infrastructure threat assessment, warning, and vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and to those involved in protecting public and private infrastructures. By visiting the DHS website (www.dhs.gov) one can quickly access any of the following DHS/IAIP products:
 - **DHS/IAIP Alerts - Advisories and Information Bulletins.** DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products are based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact.
 - **DHS/IAP Daily Open Source Infrastructure Reports.** The DHS/IAIP Daily Open Source Infrastructure Report is a daily (Monday through Friday) summary and assessment of open-source, published information concerning significant critical infrastructure issues.
 - **DHS/IAP Daily Reports Archive.** The archive allows users to access past DHS/IAIP Daily Open source Infrastructure Reports.

LEVERAGING YOUR RESOURCES

Law-enforcement professionals have limited time. Consider assigning one member of your staff to act as a point of contact with federal and state authorities, to avoid duplicate requests for information. Another approach is to have the local or statewide food-related association take responsibility for law-enforcement liaison and distribute information as it is received. Approaching federal and state agencies in a coordinated way will yield a higher level of cooperation and engagement. Local authorities (e.g., chiefs of police, sheriffs) should be contacted by local staff.

BEST PRACTICES

- Document all contacts and maintain the information provided as a permanent record.
- Use a narrative summary of the information collected to support and substantiate your assessment of a terrorism threat.
- Ensure that appropriate security is provided to safeguard threat assessment data and documents.
- Whenever possible, meet with your contacts personally. The relationships developed will be valuable in the ongoing task of developing threat assessments.
- Test the validity of positive information by checking with more than one source, if possible. This multiple-source validation process is a proven way to corroborate data. Advise law enforcement of any positive findings.

- Discuss your findings with law-enforcement authorities and report any information of concern to them.

The threat assessment allows a clearer understanding of the food organization’s vulnerabilities that might be exploited. Establishment of the threat then provides the basis for the VRA.

STEP 2: VULNERABILITY ANALYSIS

A vulnerability analysis has two essential purposes:

- Identify assets critical to the efficient and reliable performance of core business functions.
- Estimate the potential consequences associated with the loss of the function provided by the critical asset.

Critical assets include anything a food organization owns or relies upon that is absolutely essential to the conduct of its business. These assets could include facilities, plants, components, staff, raw material deliveries, information systems, data files, and support services. These critical assets are vulnerable to the extent that they can be damaged, destroyed, interrupted, or compromised in such a way that the core business functions are adversely affected.

The likelihood of an attack on a critical asset is a function of the threat combined with the vulnerability or attractiveness of the asset.

As stated above, identification of these critical assets also leads to formulation of **preventive measures** that could be implemented to reduce the vulnerability of the asset to damage. Implementing effective preventative measures ultimately reduces the risk associated with that asset.

Preventative measures can include a broad spectrum of remedies to an identified vulnerability. Such steps can include changes in administrative procedures such as:

- New employee background checks
- Employee drug testing
- Total staff security awareness training
- Reliability checks on vendors
- Standardization of plant uniforms
- Periodic computer system password changes
- Enhanced management of plant keys
- Aggressive behavior management training
- Configuration management
- Data file encryption
- Visitor Control and Identification
- Photo ID Credentials for all employees

Other preventative measures could include the familiar upgrades to a security program such as:

- Enhanced lighting
- Fence repairs and additions

- Select CCTV surveillance and recording
- Electronic facility access control
- Visual screening of critical assets
- Structural hardening of critical assets and facilities
- Firewalls

Most food organizations have an extensive body of knowledge to draw upon in performing a VRA. Designing and planning for reliable operation requires an understanding of those items that are absolutely essential to continued production. Business continuity planning often considers these types of issues, often focused on the cyber assets of the organization. Those organizations that are heavily reliant on a reliable electric power supply undoubtedly have spent considerable organizational resources on minimizing the impact of a power outage resulting from a variety of initiating events. This type of prior organizational effort can provide valuable insight in terms of identifying critical assets, potential modes of failure, potential preventative measures, damage consequences, and possible means of mitigating the consequences of asset loss. This organizational knowledge base should be augmented by the opinions of subject matter experts as well as a survey of incidents against food organizations both nationally and locally.

Critical assets are identified by answering the question, “What do I need to perform my essential core business functions?” The next step could be to break the business functions into manageable pieces such as:

- Raw material receipt
- Raw material storage
- Research and development
- Mixing
- Processing
- Packaging
- Shipping
- Utilities
- Waste Management

This functional categorization can then be further subdivided to ultimately identify those components and processes without which that functional business process cannot operate.

The vulnerability of each critical asset should be categorized as high, medium or low. This qualitative banding will be useful in determining the risk associated with each critical asset. If multiple scenarios are identified for a critical asset, the asset may also have several different vulnerabilities assigned. Another approach would be to assume the worst case scenario since it is likely that the preventative and mitigating measures will also address those scenarios of lesser consequences.

The vulnerability analysis and consequent identification of critical assets also lead to the development of associated preventative measures. Preventative measures are proactive steps taken to reduce the vulnerability of the critical assets to the postulated threat. Examples include technological security upgrades as well as procedural enhancements, all of which serve to reduce risk to the organization.

STEP 3: ESTIMATION OF CONSEQUENCES

Estimation of consequences involves predicting the impact to the food organization caused by critical asset loss or damage. Consequences can be described in various terms, including:

- Property damage, personal injury, loss of life
- Cost to repair, replace, or restore
- Lead time to repair, replace, or restore
- Loss of revenue during repair or replacement
- Downstream impact to critical customers

Similar to identification of vulnerabilities and preventive measures, consequence analysis leads to the development of **mitigating measures**. Mitigating measures include hardware, software, procedures, and staff that serve to reduce the consequences associated with the loss of, or damage to, a critical asset.

Specific damage or loss scenarios associated with each critical asset could have varying consequences; again, a conservative approach is to assume the worst-case consequences. With this approach, the risk-management strategy of the food organization will address the worst case and all lesser impacts. The list of critical assets provides a starting point for developing specific scenarios directed at those assets and resulting in either partial or complete loss of the function of that asset.

The projection and categorization of consequences should take into consideration any mitigating factors that exist at the food organization. Mitigating factors could include a large number of items, all of which would serve to reduce the consequences of an incident either in the repair, replacement, or restoration of a critical asset's function.

Looking ahead to the risk analysis (Step 4 of the VRA), the consequences associated with the loss or damage of a critical asset must be categorized as high, medium, or low. Clearly, an identical incident at two different food facilities may result in different relative consequences depending on the size of the organization, the design of the system, and the ability of each plant to restore or recover from the incident. What is important is that the consequences be categorized within the context of the specific food organization. For example, the temporary loss of a production line may be a recoverable event with minimal consequences if redundant production lines with excess capacity or emergency off-site storage of product are available. Conversely, the same event would have significant consequences if the output of the plant was dependent on the single, inoperable line. Therefore, assignment of relative consequences is a site-specific activity.

There are likely to be multiple scenarios for each identified critical asset. In general, it would be expected that the likelihood of an incident resulting in relatively low consequences would be high. Conversely, it would be expected that the likelihood of a scenario resulting in high consequences would be low. It is important to think through the various scenarios that could be directed at a critical asset and the consequences that might result from that particular scenario. In this way, various levels of mitigation can be examined and prioritized for possible implementation.

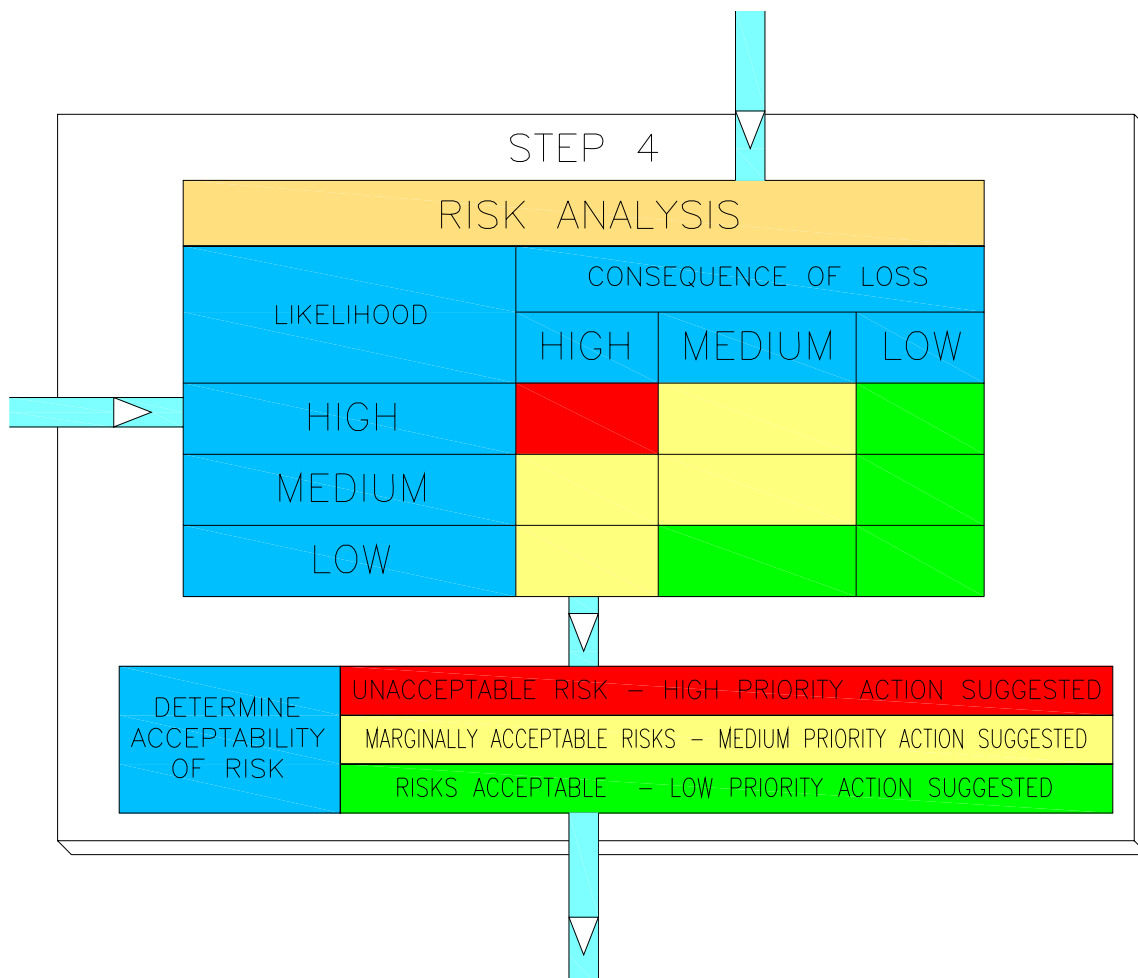
STEP 4: DETERMINATION OF RISK

Risk analysis is the qualitative combination of the likelihood of successful exploitation of a vulnerability associated with a critical asset and the consequences of that act. Likelihood, in turn, is a function of the threat and the vulnerability or attractiveness of the critical asset.

The goal of risk analysis is cost-effective reduction of overall risk to the food organization.

Once the likelihood and consequences categories have been assigned in the vulnerability analysis and consequence estimation phases, respectively, the hard work is done. These data are then combined as shown in the graphic below which is an excerpt from Figure 1 introduced earlier.

This graphic illustrates how to combine the likelihood and consequence indicators developed earlier. Very simply and as shown, a high-likelihood event with high consequences results in high risk. Conversely, low-likelihood events with low consequences result in low risk. The assignment of the high, medium, and low risk bands is based on judgment; each food organization must strategically determine what risk/likelihood combinations represent unacceptable risk.



STEP 5: IMPLEMENTATION

The final step is to prioritize for implementation and then to implement.

The risk matrix (shown in Figure 2) is an excellent tool for use in prioritizing risk management measures. The high-risk critical assets and associated scenarios represent the food organization's highest exposure to loss and therefore should be addressed first. Conversely, many low risk items can often be managed with minimal effort either through hardware, software, or procedural upgrades. As illustrated, a cost-benefit analysis can serve as a decision tool when examining specific means to address specific events. However, quantifying the risk reduction achieved for a given expenditure may be difficult and will again require common sense and good judgment.

The available risk-reduction tools are those previously listed as preventative measures and mitigation measures. The former are intended to reduce the vulnerability of the critical assets; the latter are intended to reduce the consequences of the loss of or damage to a critical asset.

Mitigating measures can be hardware, policies, procedures or software that serve to reduce:

- Loss of life or risk of injury
- Cost to repair, replace, or restore a critical asset
- Revenue lost as a result of losing the function of a critical asset

Mitigating measures can take many forms, including hardware, software, and procedures. Many organizations may already have a broad range of mitigating measures in place. Examples include:

- Maintenance of an inventory of spares used specifically in the event of loss of a critical asset
- Establishment and maintenance of mutual-aid agreements to locate and obtain spares for use in the event of the loss of critical asset
- Establishment of and training on emergency and restoration procedures in the event of loss of or damage to a critical asset
- Establishment and maintenance of information technology (IT) system backup files in the event of damage or loss of critical assets in the IT infrastructure
- Establishment of warm or hot standby IT assets to be used in the event of the loss of a critical IT infrastructure component
- Establishment of an alternate business office location in the event of loss or use of the headquarters facility
- Establishment of off-site storage of product to buffer production downtime.

ONGOING SECURITY AWARENESS

The VRA is a snapshot of a food organization's exposure to loss. This analysis should be updated as significant changes are made to the organization's systems or processes. An organization's risk can also change as a result of changes in the threat environment; therefore, plant and corporate staff should be vigilant for changes that would indicate a change in the threat to the food infrastructure and take appropriate actions. For example:

- If there is a general elevation of the Department of Homeland Security color-coded threat level, elevate your threat level one step.
- If there is a specific threat to the food industry, elevate your threat level two steps.
- If there is an attack on the food industry, elevate your threat level two steps.

Information on the threat to the food infrastructure in general can be obtained at the Food and Agriculture Information Sharing and Analysis Center at www.fmi.org/isac/.

Food organization staff should also be watching for indicators of a change in the local threat. If the following facility-specific indicators are present, consider your threat **Severe**, implement your highest level of security, and immediately notify the Federal Bureau of Investigation and local law enforcement agencies.

- Attempts to test or conduct reconnaissance of security operations at plant facilities, key resource facilities, high-profile venues or sector-specific events
- Any persons showing uncommon interest in security measures or personnel, entry points, access controls, or perimeter barriers such as fences or walls
- Any persons showing uncommon interest in food infrastructure facilities, or key resource facilities (e.g., photographing or videotaping assets)
- Theft of or missing company identification documents, uniforms, credentials, or vehicles necessary for accessing food facilities, key resource facilities or sector-specific events
- Suspicious attempts to recruit employees or persons knowledgeable about key personnel or food infrastructure facilities, key resource facilities, networks or systems
- Theft, purchase, or suspicious means of obtaining sensitive or physical security information (e.g., plans, blueprints, alarm system schematics) for food infrastructure or key resource facilities and systems
- Discovery of documents (particularly foreign-language product) containing pictures or drawings of food infrastructure or key resource facilities or systems
- Persons near food infrastructure or key resource facilities who do not fit the surrounding environment, such as individuals wearing improper attire for conditions or not normally present in the area (e.g., homeless persons, street vendors, demonstrators, or street sweepers)
- Pedestrian surveillance near food infrastructure or key resource facilities involving any surveillance activities of sensitive operations, including photography, videotaping,

extensive note-taking/ use of an audio recorder (regardless of the number of individuals involved), or mobile surveillance by cars, trucks, motorcycles, boats, or small aircraft

Adapted from the joint BI/DHS memorandum "Suspicious Activity Reporting Criteria for Infrastructure Owners and Operators," August 3, 2004

ADDITIONAL RESOURCES

THREAT ASSESSMENT RESOURCES

These Web-based resources offer both general and specific information concerning terrorism and terrorist groups.

- The National Memorial Institute for the Prevention of Terrorism (MIPT) is a non-profit organization dedicated to preventing terrorism on U.S. soil or mitigating its effects. MIPT was established after the April 1995 bombing of the Murrah federal building in Oklahoma City. This is an excellent resource for general information on terrorism in the United States, the ideology and motivation of terrorist groups, and research into terrorism prevention and mitigation. The MIPT Terrorism Knowledge Base supports searches based on terrorist groups, ideology and location. www.mipt.org
- The Anti-Defamation League (ADL) is an excellent resource for tracking extremism in the United States, including extremism in the news and politically or socially motivated violence by state. ADL's Law Enforcement Agency Resource Network (L.E.A.R.N.) and its associated newsletter are particularly useful. www.adl.org
- The Department of Homeland Security (DHS) produces a variety of resources, including important threat advisories and bulletins. In addition, the DHS Information Analysis and Infrastructure Protection (IAIP) provides a range of bulletins and advisories of interest to information-system security professionals and those involved in protecting public and private infrastructures. www.dhs.gov
- The Federal Bureau of Investigation (FBI) is the lead counterterrorism agency in the United States. Infragard, an FBI-sponsored collaboration with the private sector, works to enhance the security of critical components of the infrastructure. Food industry representation in Infragard is strongly recommended. In addition, some FBI field offices have terrorism working groups. The website provides contact information for each field office. www.fbi.gov
- LexisNexis® is an excellent subscription database service with extensive holdings and a powerful search engine. Documents may be purchased a la carte for a nominal fee. It is ideal for searching open-source media reporting and legal filings. www.lexisnexis.com