FoodQuestTQ

The TQ stands for threat quotient

MANAGING FOOD DEFENSE RISK

This paper provides an overview of the application of the CSM Method® to determine the specific food defense: 1) threats to the food supply; 2) vulnerabilities to the food supply, and; 3) countermeasures that can reduce the risk exposure of food companies to each of the identified threats and vulnerabilities. The CSM Method® is a patented process used for the protection of critical infrastructures including food and agriculture. The results of the analysis of a large data repository of all hazards events affecting the food supply and open source intelligence are presented. The results of the data analysis are used to determine what needs to be protected, why it needs to be protected and what it needs to be protected against. The clustering of events most commonly affecting the food supply and the characteristics of the potential perpetrators of food defense events are identified along with the seven essential elements of a comprehensive food defense threat statement. The five essential elements of an effective food defense program are presented. The paper concludes with a brief description of technology advances that can help the food industry balance the costs of operations with the right combination of food defense prevention and response risk countermeasures to maintain their economic viability while simultaneously reducing and maintaining their food defense risk exposure at manageable levels.

Food DefenseTQ Technical Paper No. 5

December 2012

This paper is copyrighted and should not be reproduced or copied without the express written permission of FoodQuestTQ LLC. This paper conveys no guarantees expressed or implied with respect to its content, uses and applications. The techniques described herein are an expression of the Complexity Systems Management Method or CSM Method®. The CSM Method® is owned exclusively by Projectioneering LLC and is a protected business process and data transformation patent for dealing with complex and evolving risks and risk countermeasures across all critical infrastructures (USPTO Patent No.: US 8,103,601 B2, DOI: January 24, 2012). Any questions or requests for further details regarding the POISON^{TM} food event data repository, Food Defense Architect^{TM} and other FoodQuestTQ LLC software tools should be directed to Mr. Bruce Becker at Food QuestTQ LLC on telephone 540-645-1050 or by e-mail at: http://www.bbecker@foodquesttq.com.

FoodQuestTQ LLC is located at 4720 Hayward Road, Suite 104, Frederick, Maryland 21702. Please contact us at 240-439-4476 for permission to reproduce or copy this document.

MANAGING FOOD DEFENSE RISK: Technical Paper No. 5

By John Hnatio, Chief Science Officer, FoodQuestTQ LLC

Executive Summary

The food supply is one of the most exposed of all industry verticals to risk. From fires and arson, explosions, natural disasters, workplace violence, food safety, cyber-threats, food fraud, equipment malfunction, industrial accidents, tampering and many others, the list of threats and vulnerabilities is long.

When we looked across the available literature on threats and vulnerabilities to the food supply we found that it was almost exclusively anecdotal. Since 9-11, the principal focus of government efforts appears to be directed to the low probability, high consequence threat posed by terrorist cells using intelligence tradecraft. The principal threat of concern is the undetected placement of a biological agent in large batches of food at large food processing facilities resulting in mass deaths. But the reality is that the food defense threat and vulnerability spectrum is much broader and includes arson, facility sabotage, cyber-attack, bombings, workplace violence as well as many other serious threats that can affect the economic viability of a food company, curtail production and result in severe disruption.

Since no comprehensive industry or government statement of the food defense threat to the food supply exists in the open literature, we undertook a systematic process to develop one.[i] A comprehensive threat statement tells you what needs to be protected, why it needs to be protected, and what it needs to be protected against. A clear and unambiguous statement of the threat is an essential first step before you can conduct any meaningful assessment of your vulnerabilities. Using a large food event data repository called POISON™ in combination with an extensive open source intelligence review of food events we identified the three threats and the seven essential elements that must be addressed by a comprehensive food defense threat statement.

Under the threat posed by intentional poisoning we identified the intentional poisoning of food and water by introducing physical hazards, chemical toxins, biological agents or nuclear materials into food and water and the intentional distribution, sale or use of adulterated, mishandled, and/or mislabeled food and water product. Under the threat posed by the loss of production capacity we identified fixed site facility and cyber sabotage. Under the threat posed by disruption we identified inconvenience, economic losses and fear of the population to consume food.

A comprehensive threat statement must also include a description of the capabilities of potential adversaries. This is essential in order to determine the adequacy of food defense risk countermeasures against different threats and the vulnerabilities they pose. Our analysis of food defense events in the POISON food event data repository in combination with open source intelligence analysis indicates that high consequence food defense events will be motivated by disruption. ***The following spectrum of adversary characteristics and capabilities were identified: 1) an employee insider with access, opportunity and knowledge; 2) one or more outsiders that may, or may not, have insider assistance, and; 3) organized terrorist cells using intelligence tradecraft.***

Using this statement of the threat to the food supply, a vulnerability assessment of the food supply chain was conducted. All segments of the food supply chain were found to have significant food defense vulnerabilities across one of more of the following six areas of concern: 1) the intentional introduction of harmful materials into food; 2) the intentional distribution, sale or use of spoiled, adulterated or mishandled food product; 3) intentionally mislabeled food product and other forms of food fraud; 4) the sabotage of fixed site facilities; 5) cyber-sabotage, and; 6) attacks against food operations personnel including walk-in retail customers.

Based on the results of the vulnerability assessment, specific risk reduction countermeasures were identified. This was done by reviewing the open literature and extracting global, U.S. Government and industry standards, i.e., food safety and defense schemas, related the food defense vulnerability identified. The review identified a total of 1,574 food defense related risk countermeasures.

Each of the 1,574 food defense risk countermeasures was then statistically weighted by teams of scientists, engineers and food defense experts in order to determine its risk reduction value in: 1) deterring the human actions leading to a food defense event; 2) detecting the actions of a perpetrator soon enough to prevent the food defense event; 3) preventing the event before it occurs; 4) responding to a food defense event after it has happened, and; 5) mitigating the consequences of the event. Each countermeasure was weighted in this way to determine the risk reduction value of any given food defense risk countermeasure in relation to others. ***This allows for the selection of the most effective countermeasure(s) to reduce the risk posed by a specific vulnerability.***

Finally, the 1,574 food defense countermeasures were grouped into individual areas of concern across the following five categories of food defense interest. ***The following five categories of food defense interest represent the basic components of any robust food defense plan: 1) preventing the destruction and sabotage of critical facilities and equipment; 2) protecting facility personnel; 3) preventing the intentional poisoning of food and water; 4) responding to food and facility emergencies, and; 5) building a continuity of operations plan.***

With a fundamental understanding of: 1) the threats to the food supply chain (including the characteristics of potential adversaries); 2 the vulnerabilities associated with the threats, and; 3) the value of food defense risk reduction countermeasures, an advanced computer software tool known commercially as ***Food Defense Architect^{TM} was developed to reduce food defense risk and increase cost efficiency by identifying the right combination of low cost prevention and response risk reduction measures.***

Introduction

In this paper, we treat risk management holistically as a portfolio of different risk factors that can result in untoward events. The term “all-hazards events” is used to describe the portfolio of risk factors that can impact a food company. All-hazards events include fires, explosions; site, facility and product sabotage; cyber sabotage; the intentional poisoning of food and water, the protection of facility personnel, including retail customers, and natural hazards emergencies.

The different risk factors that can impact food businesses along the supply chain are considered in the context of all-hazards events because all of the risks faced by the food industry are interconnected and interdependent. For example, you can never have a robust food defense program unless you already have an effective food safety program upon which to build it. Likewise, any robust food safety program must contain elements of food defense. We all know that fires can certainly affect food safety. But arson is the number one cause of fires in the United States. The result is that the very same investments we make to protect our facilities and equipment from industrial fires is also used to protect us from intentional arson.

This “interconnectedness” of risk factors means that the investments a food company makes in updating things like their HACCP plans should have appreciable value in strengthening their food defense plan. Likewise, a food defense vulnerability assessment should have appreciable value in strengthening a company’s HACCP plan. The evacuation drills we conduct to protect our workers from fire should also have value in protecting personnel from bomb threats and explosions and natural disasters and so on. ***The premise of this paper is that significant cost efficiencies can be achieved by leveraging this “interconnectedness” among different risk reduction factors.***

A Three Step Process: Step 1

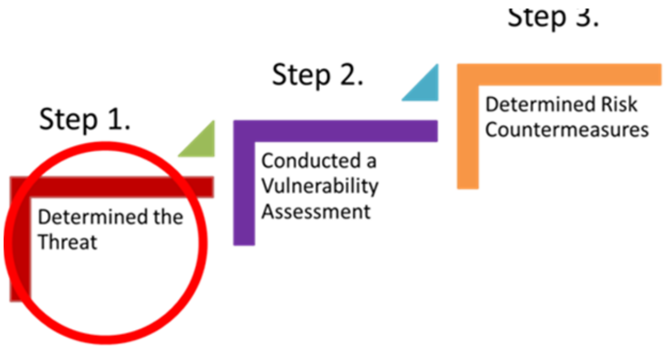

Step 1.
Determined the Threat
Step 2.
Conducted a Vulnerability Assessment
Step 3.
Determined Risk Countermeasures

Figure1: Determining the Threat

To approach the challenge of food defense, we did three things in sequential order. First, we determined the threats to the food supply. There is a great deal of information out there but most of it is spread among a huge variety of sources and is almost exclusively anecdotal. We found that much of the threat information at the government level is focused on the notion of low probability-high consequence events based on concerns about what terrorists might do. At the food industry level, we found a more traditional approach to risk management that was focused on the types of food defense risks that food related operations have to manage every day. Things like disgruntled employees who contaminate food, steal company property and misuse computers, unreliable suppliers, hijacked trucks, tampering and a host of other problems that range from medium to high probability and medium to high consequence food defense events.

To determine in a non-subjective way the threat to the food supply, we gathered information about the different types of events that occur at food facilities and created a large data repository known as POISON™. POISON covers intentional and accidental food poisonings, sabotage against food facilities and equipment, arson, fires, explosions, workplace violence, natural disasters and other all-hazards events that have disrupted the food supply. After pulling the events together from POISON and open source intelligence harvesting and analysis, we found five clusters where the events involving food facilities were concentrated: 1) arson and fires; 2) sabotage; 3) poisonings; 4) transport security, and; 5) personnel security.[ii]

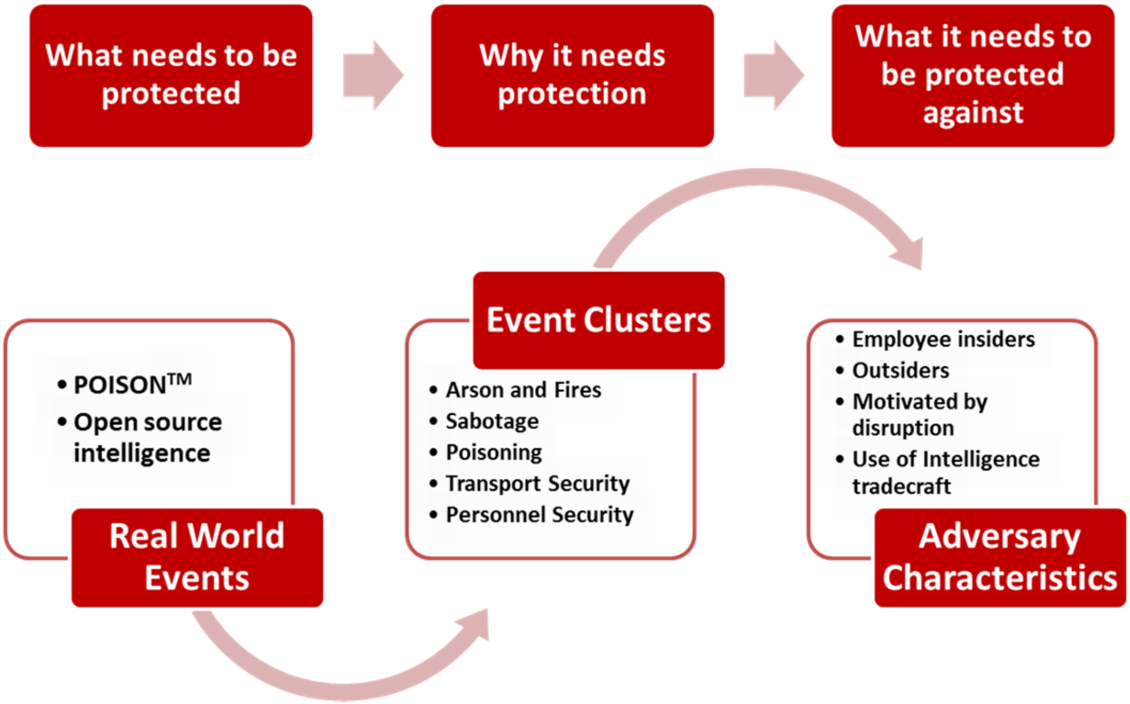


Figure 2: Defining the Food Defense Threat

A comprehensive threat statement must also include a description of the capabilities of potential adversaries. This is essential in order to determine the adequacy of food defense countermeasures against different threats and the vulnerabilities they pose. Our analysis of food defense events in the POISON food event data repository in combination with open source intelligence analysis indicates that high consequence food defense events will be motivated by disruption. The following spectrum of adversary characteristics and capabilities were identified: 1) an employee insider with access, opportunity and knowledge 2) one or more outsiders that may, or may not, have insider assistance; 3) organized terrorist cells using intelligence tradecraft.

The next step we took was to come up with the elements of a threat statement that would apply across all of the potential threats to the food industry that we found as we analyzed the events in POISON and open source intelligence. The challenge was to unambiguously state what needs to be protected, why it needs to be protected, and what it needs to be protected against.[iii]

Based on our analysis, we identified seven critical elements that should be included in a comprehensive food defense threat statement. To address the potential of intentional food poisoning, we identified the first two critical elements. The first element addresses the intentional poisoning of food by introducing physical hazards or toxic chemicals, biological agents or nuclear materials into food. The second element involves the intentional distribution, sale or use of adulterated, mishandled, and/or mislabeled food product. To address the threat of loss of production capacity, the analysis demonstrates that the third element that must be included in any comprehensive threat statement is fixed site facility sabotage. The fourth element addresses the possibility of cyber-sabotage.

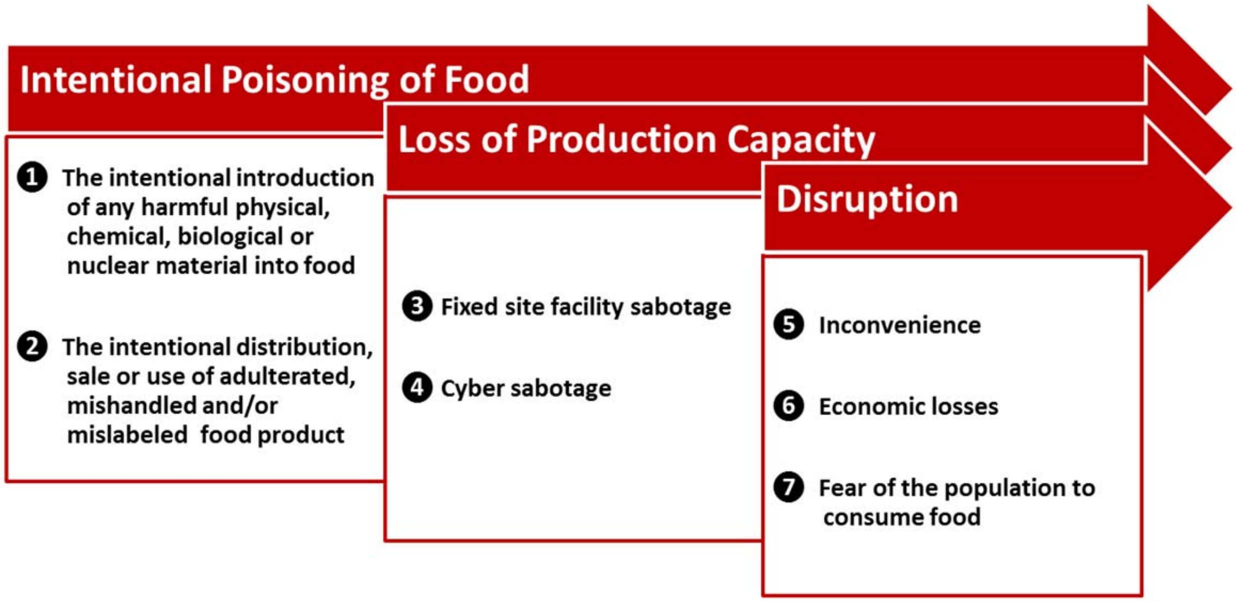

Intentional Poisoning of Food
❶ The intentional introduction of any harmful physical, chemical, biological or nuclear material into food
❷ The intentional distribution, sale or use of adulterated, mishandled and/or mislabeled food product
Loss of Production Capacity
❸ Fixed site facility sabotage
❹ Cyber sabotage
Disruption
❺ Inconvenience
❻ Economic losses
❼ Fear of the population to consume food

Figure 3: The Seven Elements of the Food Defense Threat

To address the types of disruption that would occur based on the intentional poisoning of food and loss of production capacity, the analysis shows that inconvenience, economic losses, and fear of the population to consume food must also be included as part of a comprehensive statement of the food defense threat.

A Three Step Process: Step 2.

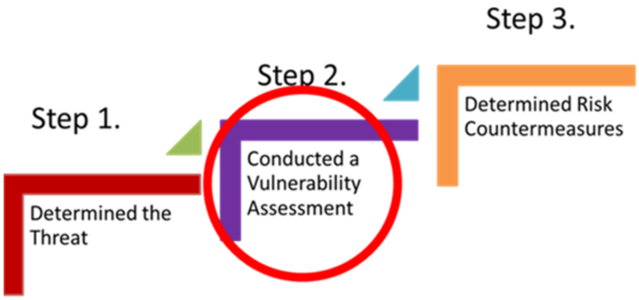
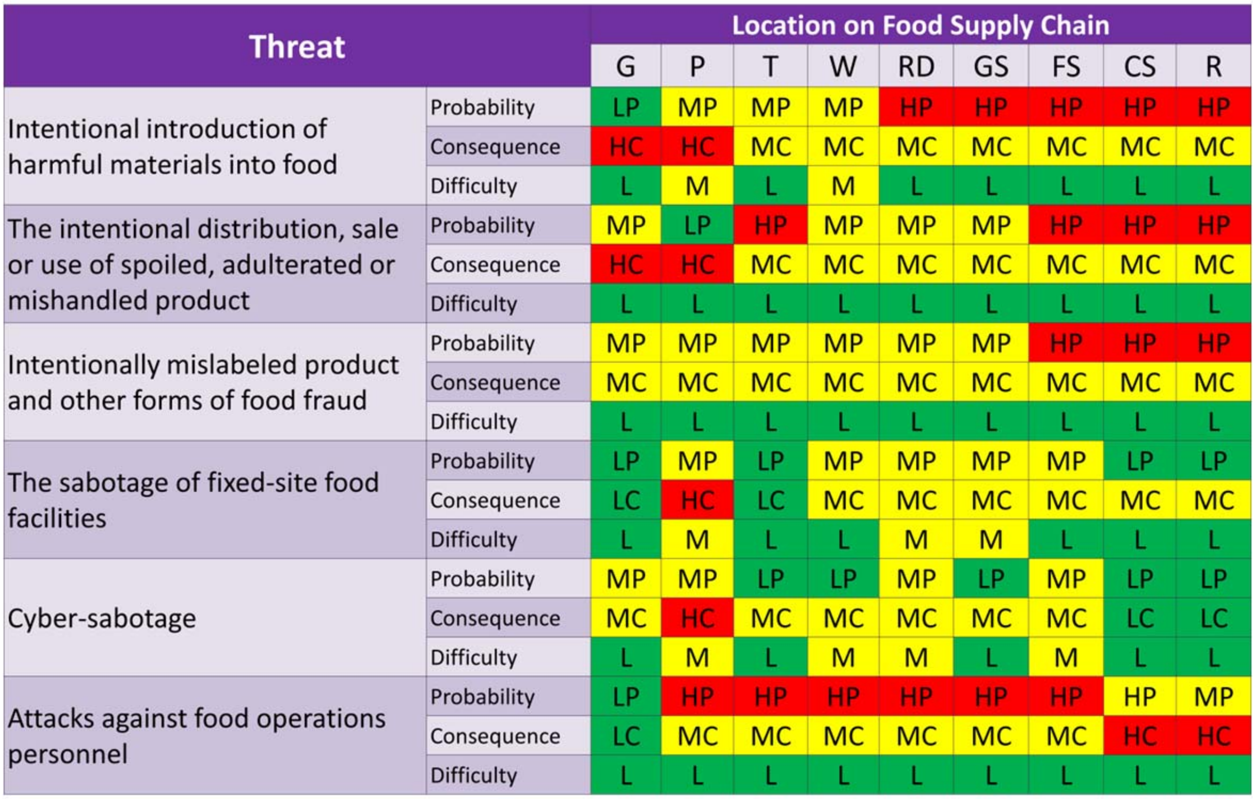

Step 1.
Determined the Threat
Step 2.
Conducted a Vulnerability Assessment
Step 3.
Determined Risk Countermeasures

Figure 4: Conducting the Vulnerability Assessment

After we determined the threat to the food supply, we were ready to move to the second step of the process. We needed to conduct a vulnerability assessment of the food supply against the design threat we developed in Step 1. We knew that without a design threat that tells you what you need to protect, why you need to protect it, and what you need to protect it against, you cannot possibly conduct a vulnerability assessment. This is because any effective vulnerability assessment must address each of the threat elements identified in Figure 3 (see page 7) and must consider the capabilities of the different types of adversaries who may attempt to take advantage of them.[iv]

After we defined what needs to be protected, why it needs to be protected, and what it needs to be protected against in a comprehensive statement of the threat to the food supply, we determined the vulnerabilities within the types of different food operations along the food supply chain. We looked across food growers (G), processors (P), transporters (T), warehouses (W), retail distributors (RD), grocery stores (GS), food service (FS), convenience stores (CS) and restaurants (R). The five clusters of events we found during our analysis of food events in POISON and from the open source intelligence review appearing in Figure 2 (see page 6) were used as threat categories. Based on the growing incidence and seriousness of computer-attacks that were found in conducting the open source intelligence analysis we identified and added the sixth cluster of cyber sabotage.



Threat		Location on Food Supply Chain								
		G	P	T	W	RD	GS	FS	CS	R
Intentional introduction of harmful materials into food	Probability	LP	MP	MP	MP	HP	HP	HP	HP	HP
	Consequence	HC	HC	MC	MC	MC	MC	MC	MC	MC
	Difficulty	L	M	L	M	L	L	L	L	L
The intentional distribution, sale or use of spoiled, adulterated or mishandled product	Probability	MP	LP	HP	MP	MP	MP	HP	HP	HP
	Consequence	HC	HC	MC	MC	MC	MC	MC	MC	MC
	Difficulty	L	L	L	L	L	L	L	L	L
Intentionally mislabeled product and other forms of food fraud	Probability	MP	MP	MP	MP	MP	MP	HP	HP	HP
	Consequence	MC	MC	MC	MC	MC	MC	MC	MC	MC
	Difficulty	L	L	L	L	L	L	L	L	L
The sabotage of fixed-site food facilities	Probability	LP	MP	LP	MP	MP	MP	MP	LP	LP
	Consequence	LC	HC	LC	MC	MC	MC	MC	MC	MC
	Difficulty	L	M	L	L	M	M	L	L	L
Cyber-sabotage	Probability	MP	MP	LP	LP	MP	LP	MP	LP	LP
	Consequence	MC	HC	MC	MC	MC	MC	MC	LC	LC
	Difficulty	L	M	L	M	M	L	M	L	L
Attacks against food operations personnel	Probability	LP	HP	HP	HP	HP	HP	HP	HP	MP
	Consequence	LC	MC	MC	MC	MC	MC	MC	HC	HC
	Difficulty	L	L	L	L	L	L	L	L	L

Figure 5: Threat Probability, Consequence and Difficulty Rankings

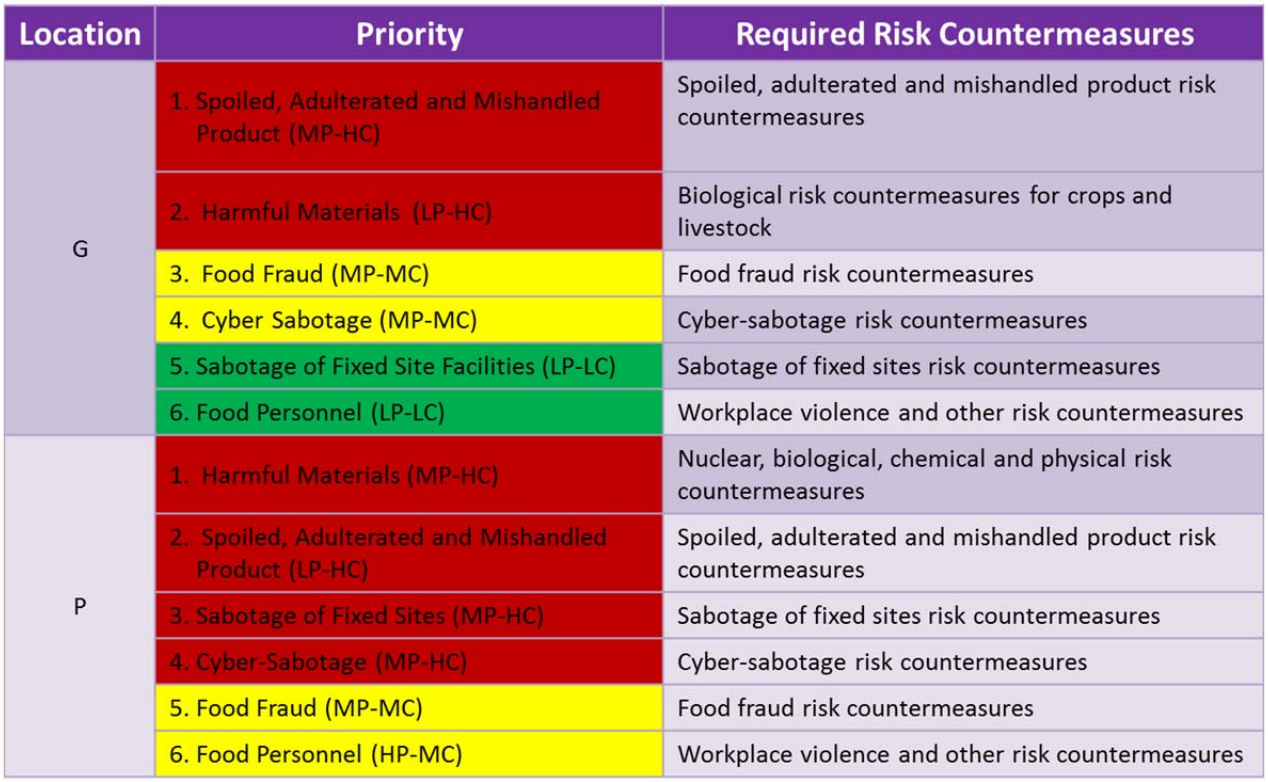
A traffic light approach of red to represent high, yellow to represent medium and green to represent low is used to signify the probability, consequence and difficulty associated with the different clusters of events across each segment of the food supply chain. Difficulty means the motivation, access to the materials necessary to mount a successful attack, and the know-how to plan and execute a successful attack. The probability of the event occurring is based on data in POISON and the analysis of open source intelligence including financial losses resulting to the food industry.[v] Past events of a similar nature in POISON and the analysis of open source intelligence (including economic losses) were used to estimate consequence.[vi] Knowledge of adversary motivation, access to the materials to carry out an attack and know-how to estimate the difficulty of attacking the different segments along the supply chain were drawn from open source intelligence analysis and used to assign a “difficulty” benchmark.

As part of the vulnerability assessment, events from the POISON database and from open source intelligence were analyzed and used to assign probability of occurrence and consequence rankings for the introduction of harmful materials, the distribution and sale of spoiled, adulterated and mishandled product, intentional mislabeling and other forms of food fraud, the sabotage of fixed site facilities, cyber-sabotage and the protection of food operations personnel including retail customers.

A traffic light approach was used to signify levels of concern. Red indicates the highest level of concern. All threat events with a high consequence, regardless of their probability of occurrence are marked in red. For example, even though the probability of someone intentionally introducing foot and mouth disease at several U.S. beef farms is low, the consequences could have a devastating impact on the beef industry and U.S. agricultural exports. In another example, even though the probability that a terrorist group could successfully introduce enough of the right toxin or biological agent into a large enough food batch to result in a catastrophic outcome is low, the consequences of a successful attack could have devastating consequences. In a final example, although the probability that an act of violence will occur at a retail distributor, grocery store, convenience store and a restaurant ranges from low to medium probability of occurring, the results have proven to be devastating in terms of loss of life and brand name risk exposure for many of the companies involved, so they appear in red. In similar fashion, yellow represents a very serious level of concern. All medium consequence events appear in yellow. Yellow signifies that while the impact of such an event would have very serious consequences on the company involved the outcome is still manageable. Green signifies that the event is manageable. All low consequence events appear in green. Green signifies that while such an event will adversely impact the company involved, the outcome is manageable.

In the following series of figures we show, in rank order, the specific threats of concern to food growers (G), processors (P), transporters (T), warehouses (W), retail distributors

(RD), grocery stores (GS), food service (FS), convenience stores (CS) and restaurants (R) and the associated risk countermeasures that should be emphasized.

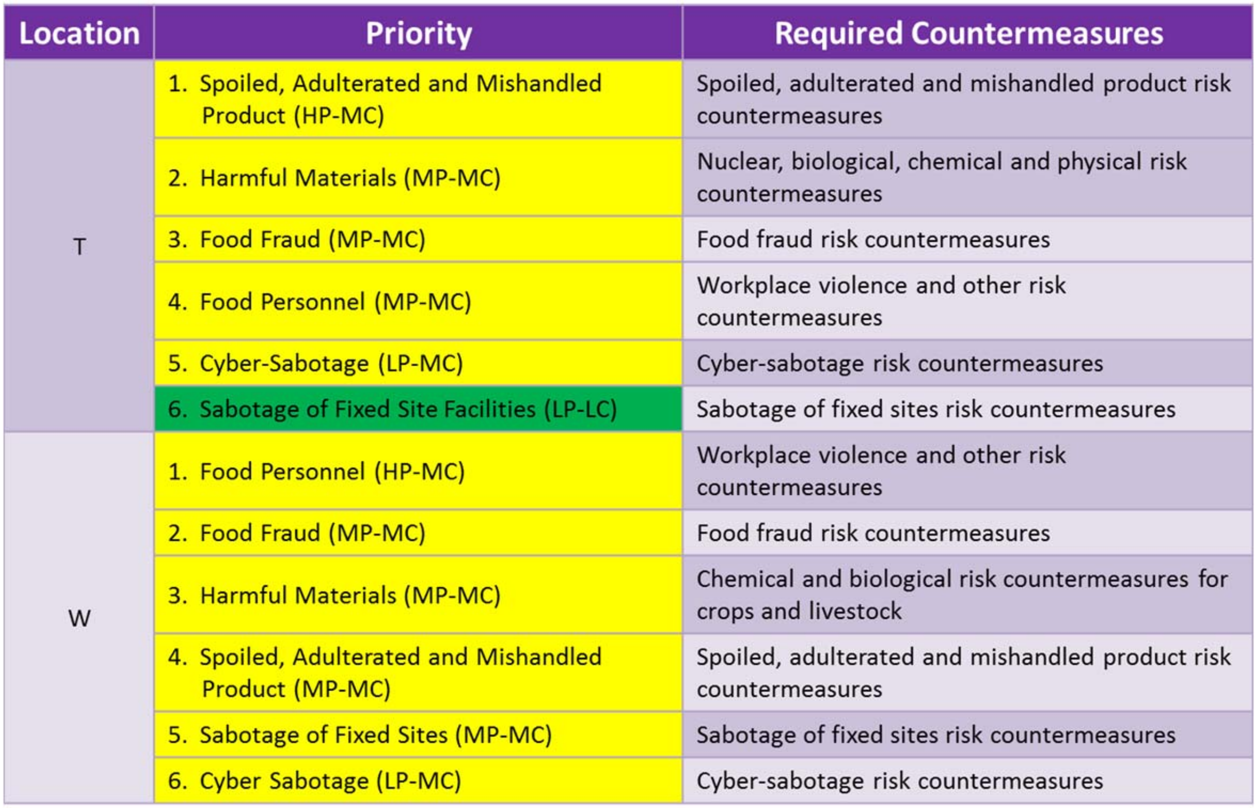


Location	Priority	Required Risk Countermeasures
G	1. Spoiled, Adulterated and Mishandled Product (MP-HC)	Spoiled, adulterated and mishandled product risk countermeasures
	2. Harmful Materials (LP-HC)	Biological risk countermeasures for crops and livestock
	3. Food Fraud (MP-MC)	Food fraud risk countermeasures
	4. Cyber Sabotage (MP-MC)	Cyber-sabotage risk countermeasures
	5. Sabotage of Fixed Site Facilities (LP-LC)	Sabotage of fixed sites risk countermeasures
	6. Food Personnel (LP-LC)	Workplace violence and other risk countermeasures
P	1. Harmful Materials (MP-HC)	Nuclear, biological, chemical and physical risk countermeasures
	2. Spoiled, Adulterated and Mishandled Product (LP-HC)	Spoiled, adulterated and mishandled product risk countermeasures
	3. Sabotage of Fixed Sites (MP-HC)	Sabotage of fixed sites risk countermeasures
	4. Cyber-Sabotage (MP-HC)	Cyber-sabotage risk countermeasures
	5. Food Fraud (MP-MC)	Food fraud risk countermeasures
	6. Food Personnel (HP-MC)	Workplace violence and other risk countermeasures

Figure 6: Rank Order of Threat Concerns for Growers and Processors

The occurrence of major food poisoning incidents and the introduction of spoiled, adulterated or mishandled product leading to criminal indictments and civil litigation for negligence have become major concerns for growers. In a growing number of cases, serious poisoning incidents have forced these companies into bankruptcy. For growers, the introduction of the right type of undetected toxin or biological agent into a large batch of food product could also have devastating consequences. The possibility of food fraud and cyber-sabotage (medium and large growers for traceability) would have medium consequences. The sabotage of building structures and violence against farms and farmers is considered to be a low probability and low consequence event.

Food processors have the greatest risk exposure of any single segment along the food supply chain. Although the probability is low, if the right toxin or biological agent were successfully introduced into a large batch the consequences could be devastating. In complex supply chains that allow for the fast and broad distribution of food both spoiled, adulterated and/or mishandled product and food fraud could have devastating impact on brand name. Processors are the most vulnerable to the sabotage of fixed sites with potentially devastating consequences. Cyber-sabotage could threaten food production, distribution and traceability to result in devastating consequences. Finally, the consequences of violence involving food personnel is considered as a medium consequence event due to the high cost of reparations and negative effects on employee morale and resulting decreases in production.

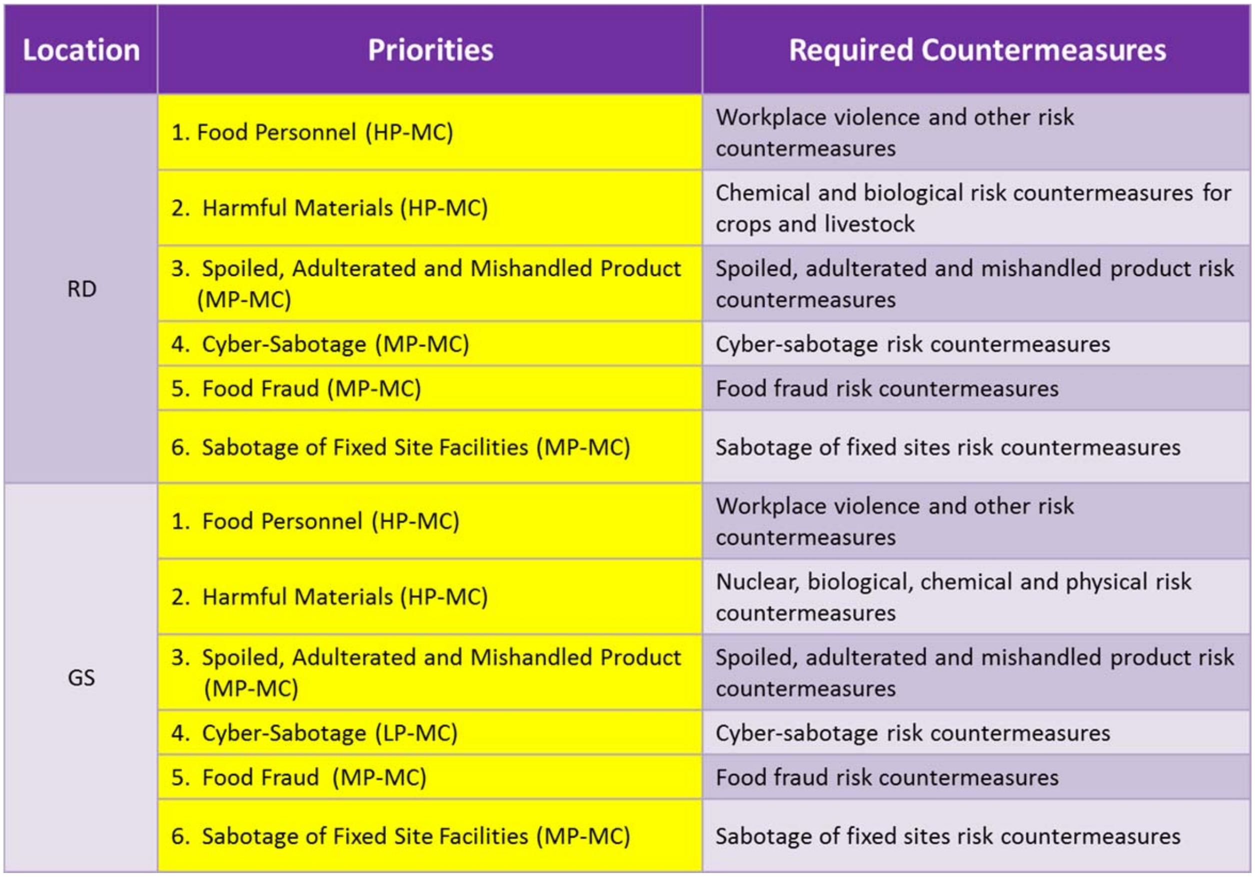


Location	Priority	Required Countermeasures
T	1. Spoiled, Adulterated and Mishandled Product (HP-MC)	Spoiled, adulterated and mishandled product risk countermeasures
	2. Harmful Materials (MP-MC)	Nuclear, biological, chemical and physical risk countermeasures
	3. Food Fraud (MP-MC)	Food fraud risk countermeasures
	4. Food Personnel (MP-MC)	Workplace violence and other risk countermeasures
	5. Cyber-Sabotage (LP-MC)	Cyber-sabotage risk countermeasures
	6. Sabotage of Fixed Site Facilities (LP-LC)	Sabotage of fixed sites risk countermeasures
W	1. Food Personnel (HP-MC)	Workplace violence and other risk countermeasures
	2. Food Fraud (MP-MC)	Food fraud risk countermeasures
	3. Harmful Materials (MP-MC)	Chemical and biological risk countermeasures for crops and livestock
	4. Spoiled, Adulterated and Mishandled Product (MP-MC)	Spoiled, adulterated and mishandled product risk countermeasures
	5. Sabotage of Fixed Sites (MP-MC)	Sabotage of fixed sites risk countermeasures
	6. Cyber Sabotage (LP-MC)	Cyber-sabotage risk countermeasures

Figure 7: Rank Order of Threat Concerns for Transporters and Warehouse Facilities

For transporters the threats posed by the introduction of harmful materials, the distribution of spoiled, adulterated and mishandled product, food fraud, cyber sabotage and driver safety issues associated with the frequency of truck hijackings are all medium consequence events. As would be expected, the probability of occurrence and consequences associated with the sabotage of fixed site facilities are low for transporters.

Warehouses face medium consequences across all six threat areas.

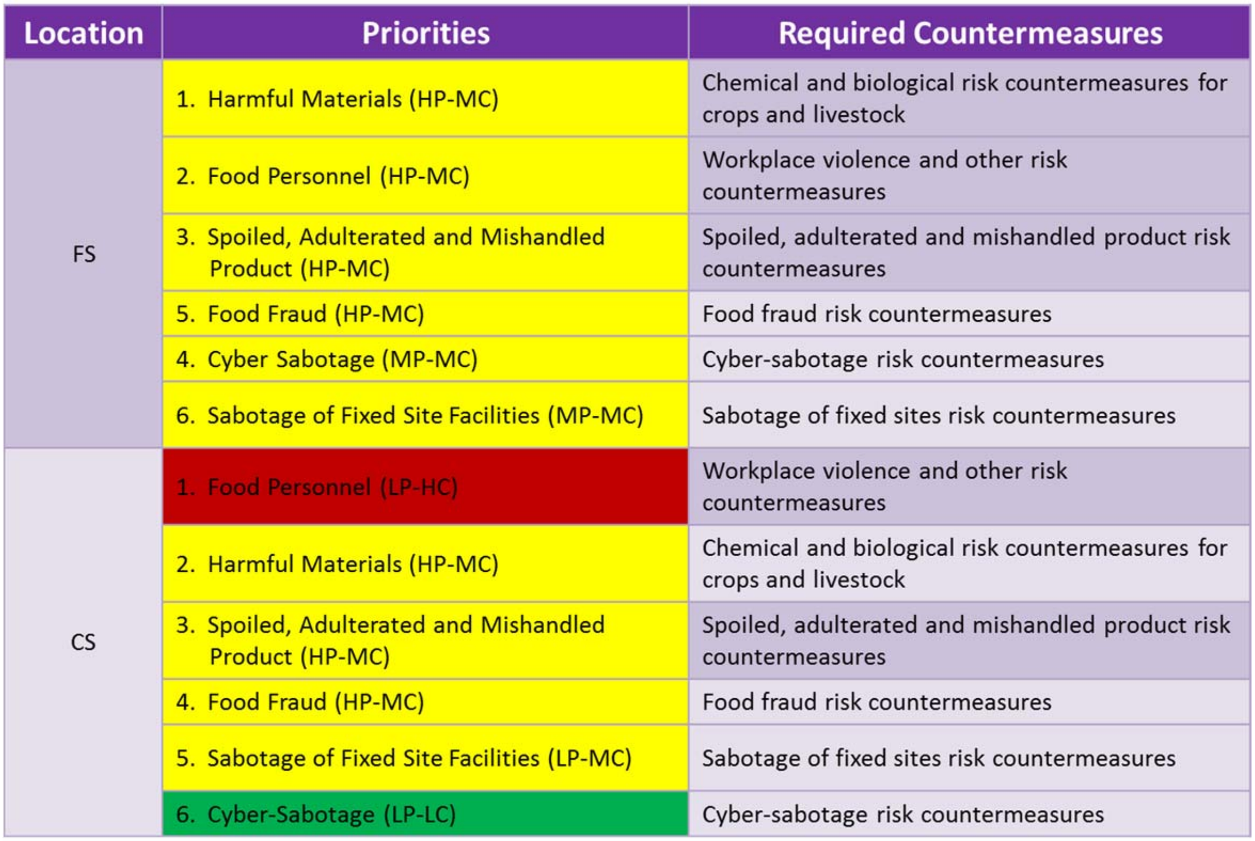


Location	Priorities	Required Countermeasures
RD	1. Food Personnel (HP-MC)	Workplace violence and other risk countermeasures
	2. Harmful Materials (HP-MC)	Chemical and biological risk countermeasures for crops and livestock
	3. Spoiled, Adulterated and Mishandled Product (MP-MC)	Spoiled, adulterated and mishandled product risk countermeasures
	4. Cyber-Sabotage (MP-MC)	Cyber-sabotage risk countermeasures
	5. Food Fraud (MP-MC)	Food fraud risk countermeasures
	6. Sabotage of Fixed Site Facilities (MP-MC)	Sabotage of fixed sites risk countermeasures
GS	1. Food Personnel (HP-MC)	Workplace violence and other risk countermeasures
	2. Harmful Materials (HP-MC)	Nuclear, biological, chemical and physical risk countermeasures
	3. Spoiled, Adulterated and Mishandled Product (MP-MC)	Spoiled, adulterated and mishandled product risk countermeasures
	4. Cyber-Sabotage (LP-MC)	Cyber-sabotage risk countermeasures
	5. Food Fraud (MP-MC)	Food fraud risk countermeasures
	6. Sabotage of Fixed Site Facilities (MP-MC)	Sabotage of fixed sites risk countermeasures

Figure 8: Rank Order of Threat Concerns for Retail Distributors and Grocery Stores

For retail distributors the priority concern is violence affecting retail establishments of all kinds.[vii] The violence may be among employees or by outsiders. The consequences of violence, especially shootings, make retail food stores extremely vulnerable to after the fact adverse brand name exposure. The introduction of harmful materials, spoiled and mishandled product, cyber-sabotage, food fraud and sabotage to fixed facilities are all considered to be medium consequence events.

Grocery stores are assigned the same ranking as retail distributors for the same reasons.

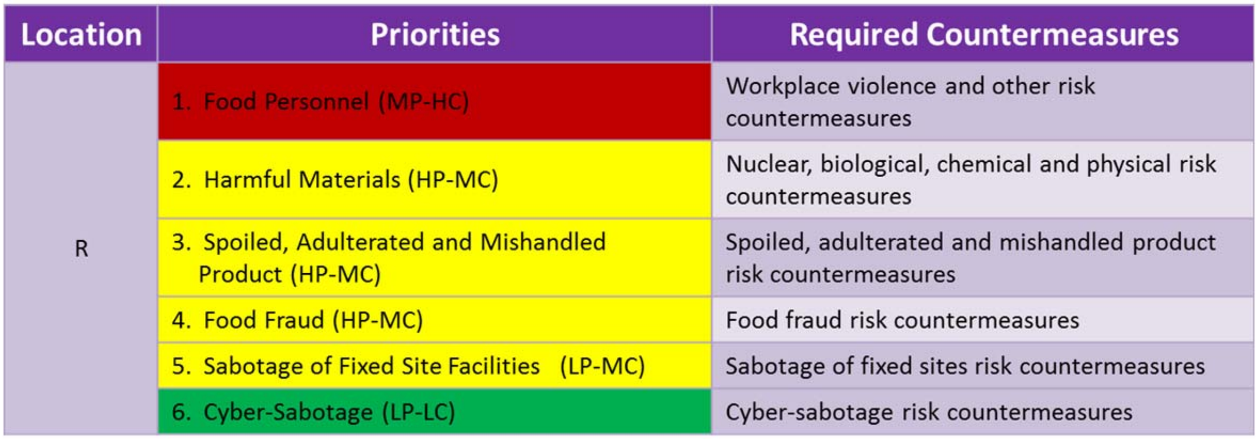


Location	Priorities	Required Countermeasures
FS	1. Harmful Materials (HP-MC)	Chemical and biological risk countermeasures for crops and livestock
	2. Food Personnel (HP-MC)	Workplace violence and other risk countermeasures
	3. Spoiled, Adulterated and Mishandled Product (HP-MC)	Spoiled, adulterated and mishandled product risk countermeasures
	5. Food Fraud (HP-MC)	Food fraud risk countermeasures
	4. Cyber Sabotage (MP-MC)	Cyber-sabotage risk countermeasures
	6. Sabotage of Fixed Site Facilities (MP-MC)	Sabotage of fixed sites risk countermeasures
CS	1. Food Personnel (LP-HC)	Workplace violence and other risk countermeasures
	2. Harmful Materials (HP-MC)	Chemical and biological risk countermeasures for crops and livestock
	3. Spoiled, Adulterated and Mishandled Product (HP-MC)	Spoiled, adulterated and mishandled product risk countermeasures
	4. Food Fraud (HP-MC)	Food fraud risk countermeasures
	5. Sabotage of Fixed Site Facilities (LP-MC)	Sabotage of fixed sites risk countermeasures
	6. Cyber-Sabotage (LP-LC)	Cyber-sabotage risk countermeasures

Figure 9: Rank Order of Threat Concerns for Food Service and Convenience Stores

Like warehouses, food service establishments face medium consequences across all six threat areas.

Convenience stores, like other food retailers, face the threat of violence against personnel. The violence is usually instigated by outsiders and robbery attempts. The consequences of violence, especially shootings, make convenience stores extremely vulnerable to after the fact adverse brand name exposure. The introduction of harmful materials, spoiled and mishandled product, food fraud and fixed site facility sabotage (not involving workplace violence) are considered to be medium consequence events for convenience stores. The probability and consequences of cyber-sabotage are considered low.



Location	Priorities	Required Countermeasures
R	1. Food Personnel (MP-HC)	Workplace violence and other risk countermeasures
	2. Harmful Materials (HP-MC)	Nuclear, biological, chemical and physical risk countermeasures
	3. Spoiled, Adulterated and Mishandled Product (HP-MC)	Spoiled, adulterated and mishandled product risk countermeasures
	4. Food Fraud (HP-MC)	Food fraud risk countermeasures
	5. Sabotage of Fixed Site Facilities (LP-MC)	Sabotage of fixed sites risk countermeasures
	6. Cyber-Sabotage (LP-LC)	Cyber-sabotage risk countermeasures

Figure 10: Rank Order of Threat Concerns for Restaurants

Finally, restaurants like other food retailers face the threat of violence against personnel and their customers. The violence is frequently instigated by outsiders and may involve mass shootings. The consequences of violence, especially shootings, make restaurants extremely vulnerable to after the fact adverse brand name exposure. The introduction of harmful materials, spoiled, adulterated and mishandled product, cyber-sabotage and food fraud are considered to be medium consequence events for restaurants. The consequences of fixed site facility sabotage (not involving workplace violence) are considered low.

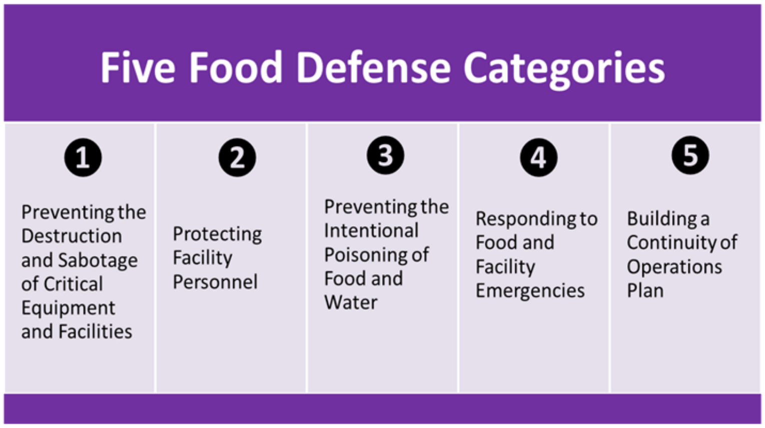

Five Food Defense Categories
1
Preventing the Destruction and Sabotage of Critical Equipment and Facilities
2
Protecting Facility Personnel
3
Preventing the Intentional Poisoning of Food and Water
4
Responding to Food and Facility Emergencies
5
Building a Continuity of Operations Plan

Figure 11: Five Food Defense Categories

As the final step in completing the vulnerability assessment of the food supply we identified five categories of interest that must be part of a comprehensive food defense plan based on the vulnerability assessment. First, a food defense program must address the sabotage of critical equipment and facilities. Second, it must protect facility personnel and walk-in retail customers from intentional attacks such as shootings, bombings, arson and other threats. Third, it must prevent the intentional poisoning of food and water. Fourth, there needs to be an effective command and control system in place to respond to food facility emergencies. Fifth, food operations must be prepared to deal with the loss of production and delivery capacity by having plans in place to shorten the curtailment of their operations.

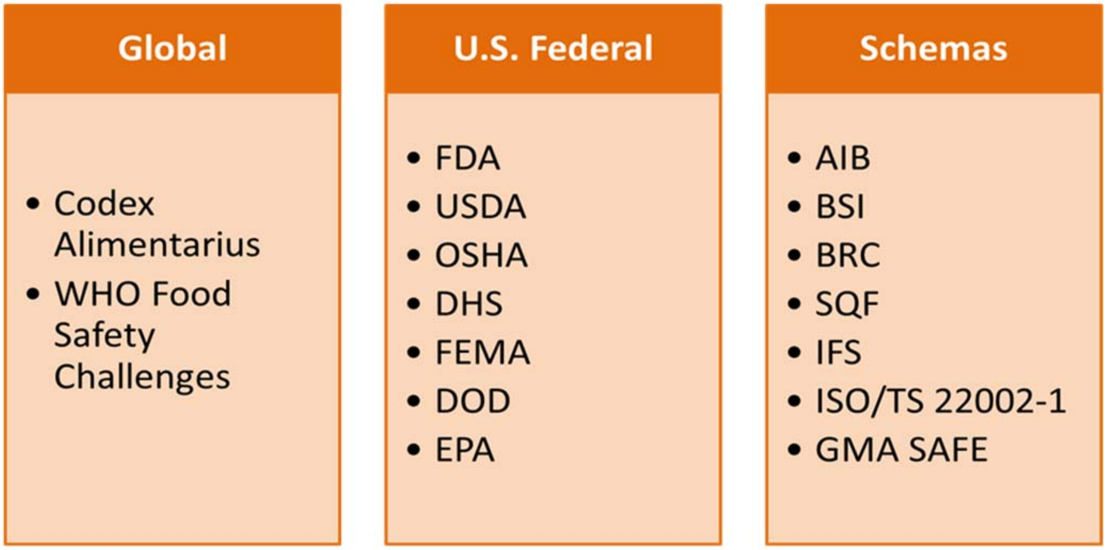
A Three Step Process: Step 3.

Step 1.
Determined the Threat
Step 2.
Conducted a Vulnerability Assessment
Step 3.
Determined Risk Countermeasures

Figure 12: Determining Risk Countermeasures

In the third and final phase of the CSM Method® we turned our attention to determining the most effective risk countermeasures that should be employed to address each of the threats and vulnerabilities that were identified in steps 1 and 2.

We started at the global level and extracted every food defense related benchmark and audit standard associated with the five categories food defense interest of: 1) the sabotage of critical equipment and facilities including cyber-sabotage; 2) the protection of facility personnel and retail customers from intentional attacks such as shootings, bombings, arson and other threats; 3) the intentional poisoning of food and water; 4) an effective command and control system must be in place to respond to food facility emergencies, and; 5) the presence of continuity of operations plans to deal with the loss of production capacity by having plans in place to shorten the curtailment of their operations. In similar fashion, every food defense and site security related standard across the U.S. Government and the seven principal industry food safety and food defense schemas were also extracted.



Global

- Codex Alimentarius
- WHO Food Safety Challenges

U.S. Federal

- FDA
- USDA
- OSHA
- DHS
- FEMA
- DOD
- EPA

Schemas

- AIB
- BSI
- BRC
- SQF
- IFS
- ISO/TS 22002-1
- GMA SAFE

Figure 13: Sources of Food Defense Related Risk Countermeasures

A total of 1,574 food defense and site security related countermeasures were identified. The countermeasures were grouped into the five food defense categories of interest that were identified as the result of the vulnerability assessment (see Figure 11). Scientists and subject matter experts used similar events in the POISON^{TM} food defense data repository and from open source intelligence to weight the value of each countermeasure in: 1) deterring the human actions leading to a particular type of food defense event; 2) detecting the actions of a perpetrator soon enough to prevent the event; 3) actually preventing the event; 4) improving the response to the event, and; 5) mitigating the consequences of the event. To do this, the scientists and food defense subject matter experts used a 5 point graduated Likert scale with their scores validated by independent peer review. In this way, the value of each food defense risk countermeasure (and combinations of countermeasures) in addressing specified threats was determined. The countermeasures with the highest scores were flagged and represent the best investments a food company can make to prevent and respond food defense threats and their associated vulnerabilities.

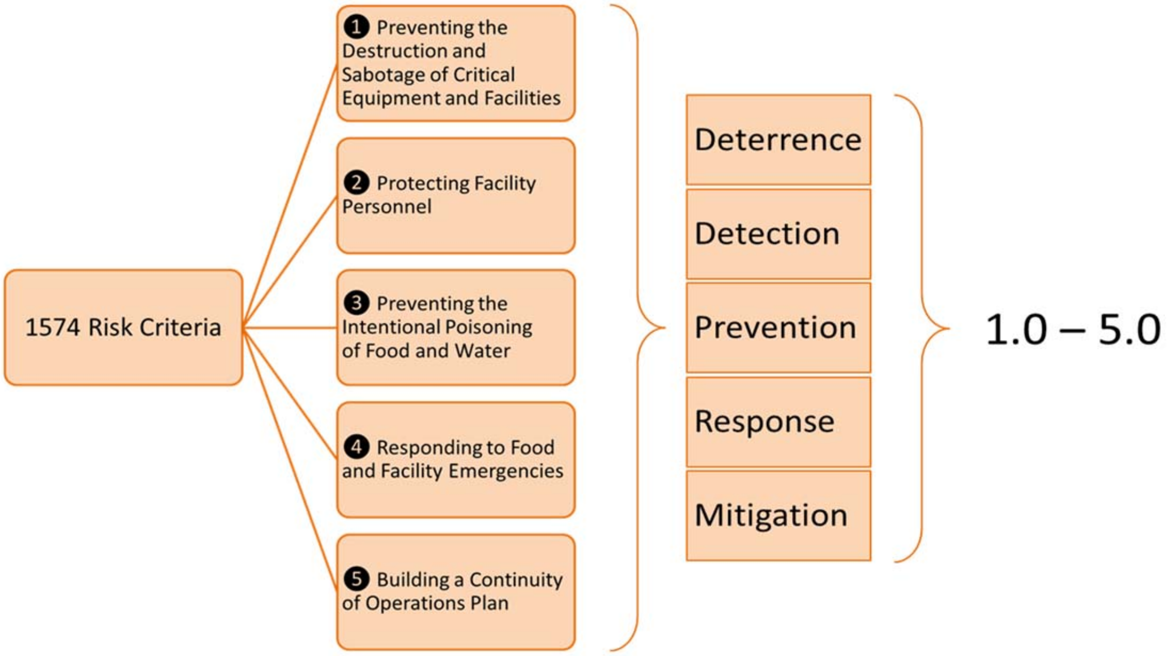

1574 Risk Criteria
❶ Preventing the Destruction and Sabotage of Critical Equipment and Facilities
❷ Protecting Facility Personnel
❸ Preventing the Intentional Poisoning of Food and Water
❹ Responding to Food and Facility Emergencies
❺ Building a Continuity of Operations Plan
Deterrence
Detection
Prevention
Response
Mitigation
1.0 – 5.0

Figure 14: Identification, Grouping and Weighting of
Food Defense Risk Countermeasures

Leveraging Technology to Achieve Food Defense Cost Efficiencies and Reduce Losses

With a fundamental understanding of: 1) the threats to the food supply chain that includes the characteristics of potential adversaries; 2) the vulnerabilities associated with the threats, and; 3) the value of food defense risk reduction countermeasures, a computer software program was developed to reduce food defense risk and increase cost efficiency by identifying the right combination of low cost prevention and response risk reduction measures that should be employed to address each vulnerability.

The software tool, which is based on the patented CSM Method®[viii], is called Food Defense Artchitect™. Food Defense Architect is a secure, cloud-based software platform that allows small, medium and large food growers, processors, transporters, warehouses, retail distributors, grocery stores, and food service companies (including caterers) to develop (and strengthen) their food defense programs to reflect their business size and location on the supply chain. The software reduces personnel time on task while simultaneously encouraging multi-disciplinary problem solving through the use of a workflow management protocol where food managers can assign different categories of questions to different operating personnel. The software is also full spectrum enabled to function on workstations, lap top computers, tablet and cell phone technology. This increases personnel cost efficiencies by allowing for both "in-the-office" and "on-the-floor" data inputs.

The software tool looks across each of the five categories of food defense interest: 1) the sabotage of critical equipment and facilities including cyber-sabotage; 2) the protection of facility personnel including retail customers from intentional attacks such as shootings, bombings, arson and other threats; 3) the intentional poisoning of food and water; 4) an effective command and control system to respond to food facility emergencies, and; 5) continuity of operations plans to deal with the loss of production capacity. It uses a questions accompanied by several steps and a "yes" or "no" format. By selecting the steps that are in place, the software generates a threat quotient. A threat quotient is the average of the deterrence, detection, prevention, response and mitigation scores for the food defense risk countermeasures, i.e., steps, which are selected.[ix]

The software also reduces the costs associated with assessments and audits through perpetual assessment. Perpetual assessment means that once the desired combination of prevention and response risk countermeasures are in place their implementation is continuously monitored by real-time feedback from operating personnel using personal digital assistants (PDA's). A cost factor analysis of food safety and food defense assessments and audits indicates that the costs associated with assessment and audits can be reduced by up to 60% through the application of perpetual assessment methods.[x]

Conclusion

The goal of risk management is to help food companies balance the cost of their operations with the right combinations of prevention and response measures that keep losses low and profits high. Thus, the cost and effectiveness of food defense risk reduction measures in preventing and responding to food defense threats and vulnerabilities must be at the heart of any successful food protection strategy.

Recent advances in science and information technology now make it possible, for the first time, to quantitatively determine the value of risk countermeasures and combinations of risk countermeasures in preventing and, when necessary, mounting the most effective responses to all-hazards risk events that can affect a food company.[xi] Using these new advances, food companies can select and put into place the most cost effective combinations of prevention and response risk countermeasures that can keep their losses low and profits high.

End Notes

[i] Complexity Systems Management Method, Patent No.: US 8,103,601 B2. Date of Issue: January 24, 2012. United States Patent and Trademark Office: Washington, D.C. Read more at: http://www.patentgenius.com/patent/8103601.html

[ii] Note: The POISON food event data repository contains 1500 selected all hazards events impacting the food supply to include accidental and intentional poisonings of food and water, fires, arson and sabotage, industrial accidents, equipment malfunction, workplace violence and natural disasters. FoodQuestTQ LLC does not publicly share our analysis of intentionally motivated attacks to avoid assisting terrorists and criminals. Read more about POISON at: http://www.nfpcportal.com/FQTools/POISON/tabid/197/Default.aspx

[iii] Jech, Ronald. (April 2010). NATO Science for Peace and Security Programme. NATO Advanced Technology Workshop: Advances in food security and safety against terrorist threats and natural disasters. Presentation, Risk management as it relates to food. Cairo, Egypt. Read more at: http://agtechint.com/uploads/Risk_Management_as_it_Relates_to_Food.pdf

[iv] Note: The public availability of a clear statement of the threats to the food supply that includes a description of the capabilities and characteristics of potential adversaries is an essential first step before the food industry can conduct effective food defense vulnerability assessments. The use of tools such as C.A.R.V.E.R. plus SHOCK in the absence of an unambiguous design basis threat can yield serious false positives with respect to the detection, prevention and effective responses to low probability-high consequence terrorist events.

[v] ThoughtQuest LLC (May 2011). Food: Market analysis and worksheets for the costing of assessments and audits and food industry losses as the result of all hazards events. ThoughtQuest LLC: Frederick, MD

[vi] ThoughtQuest LLC (May 2011). Food: Market analysis and worksheets for the costing of assessments and audits and food industry losses as the result of all hazards events. ThoughtQuest LLC: Frederick, MD

[vii] Northwood, Joyce (December 2011). Assaults and Violent Acts in the Private Retail Trade Sector, 2003—2008. Bureau of Labor Statistics, Department of Labor: Washington D.C., as retrieved from the World Wide Web at: http://www.bls.gov/opub/cwc/sh20111202ar01p1.htm

[viii] Complexity Systems Management Method, Patent No.: US 8,103,601 B2, Date of Issue: January 24, 2012. United States Patent and Trademark Office: Washington, D.C. Read more at: http://www.patentgenius.com/patent/8103601.html

[ix] Note: Read more about Food Defense Architect™ at: http://nfpcportal.com/FQTools/FoodDefenseArchitect/tabid/282/Default.aspx

[x] ThoughtQuest LLC (May 2011). Food: Market analysis and worksheets for the costing of assessments and audits and food industry losses as the result of all hazards events. ThoughtQuest LLC: Frederick, MD

[xi] Complexity Systems Management Method, Patent No.: US 8,103,601 B2, Date of Issue: January 24, 2012. United States Patent and Trademark Office: Washington, D.C. Read more at: http://www.patentgenius.com/patent/8103601.html

About the Author

John Hnatio is the Chief Science Officer at FoodQuestTQ. His career with the U.S. Government and industry spans a period of over 35 years where he has been involved in risk management. His service to the government includes threat analysis, vulnerability assessments and the implementation of risk countermeasures at U.S. nuclear weapons and other sensitive facilities, nuclear transportation systems and nuclear reactors worldwide. He also served as a loaned executive to the United States Senate from the Administration of President Ronald W. Reagan where he advised on risk matters involving the nuclear and biological programs of the former Soviet Union. In 2004, John retired from the U.S. government and is now an owner of several companies where he works with industry to reduce risk and enhance the resiliency of the nation's critical infrastructures including food and agriculture. He established FoodQuestTQ in 2011. John is the author of several patents and holds a doctorate degree from the George Washington University. He also holds a doctorate degree awarded honoris causa from the Urals Branch of the Russian Academy of Sciences.