Security and robustness in food supply chains in the Netherlands

By

Solyana A. Subuh

In Partial Fulfillment of the Award of
M Sc. in Management, Economics and Consumer Studies (MME)

Specialization:
Business Economics

Supervisors: Dr Miranda Meuwissen
Business Economics Group (BEC)

Dr Ge Backus
Agricultural Economics Research Institute (LEI)

March 2008

Acknowledgements

The completion of this thesis would not have been possible, had it not been for the assistance and cooperation I received from several individuals.

I would like first to extend my deepest gratitude to my supervisor, Dr Miranda Meuwissen for her critical comments, encouragement, and great supervisory role during the writing of this thesis. Thank you for always being so supportive and open. My sincere thanks go to Dr Ge Backus for his stimulating discussions and comments all the way from the inception of my study through the writing up of this thesis. I am also very grateful to Dr Gertjan Hofstede and Dr Paul Ingenbleek for their stimulating discussion we had especially at the initial stages of this study. I am also grateful to Manfred Hessing, Stephen Gielen and Dr Suzan Horst for their critical comments on the preparation of my questionnaire.

I would also like to thank to my beloved family and all of my friends who stood by my side during my whole course of study. I especially thank my sister Hana Berhane and my beloved brother Zenebe Abreha for their encouragement and support throughout my study.

Summary

Background

Food can be intentionally or accidentally contaminated at any time and point along the chain and the occurrence of contamination at one place could have a substantial effect on public health (WHO, 2002). In addition to the public health impacts, deliberate contamination could cause potentially large economic consequences including costs for response to an attack, disruption of food distribution and long-term loss of consumer confidence. Food safety systems such as HACCP and GMP do not specifically address the intentional contamination of food (Takhistov and Bryant, 2006). Therefore, "security systems" such as ISO28000:2005 (specification for security management systems for the supply chain) and AEO (Authorized Economic Operator) have recently been introduced, the latter only since January 1, 2008. Despite these new certification systems, recognized in a US security assessment study that areas of communication, management support and interaction with suppliers, customers and carriers are often overlooked.

The objective of the study is to explore companies' activities in preventing the risk from occurrence (risk prevention) and minimizing the size of loss after occurrence (risk mitigation). Companies' perceptions about risk prevention were captured by addressing *control actions* taken and *information sharing* practices employed. Risk mitigation, or, *robustness*, was addressed by investigating companies' emergency plans and budgets. An extensive literature was reviewed to get insight into the concepts raised in this study and in order to elicit companies' perceptions about their security performance a semi-structured questionnaire was developed. Companies involved have (part of) their business in the Netherlands and are from the meat and vegetable supply chains.

Risk prevention

Companies hardly share information with suppliers and consumers regarding intentional contaminations. Information sharing practices that are more closely related to food safety assurance, such as implementing information systems, maintaining records on company's production processes, sharing sources of products, tracking and tracing, and recall procedures are well undertaken.

With regard to control actions findings are somewhat similar as for the information sharing practices: control actions that have close relationship with food safety issues such as assigning responsibility to qualified individuals and restricting access to key facilities and sensitive areas are well undertaken. Security related practices, such as assigning senior management position focusing on security, use of RFID and other technologies to verify container contents, inspecting suppliers' plants are not well undertaken. HACCP is considered as the main guideline and certification scheme to prevent intentional contaminations. Security specific certifications such as ISO28000:2005 and guidelines issued by FDA and USDA FSIS are not implemented.

Risk mitigation

Robustness seems to better organized at company level (i.e. when there is a lack of facilities) than at supply chain level (i.e. at times of lack of raw material).With regard to emergency budget companies do not seem to agree to maintain emergency budgets to carry on operations after occurrence of the risk.

Performance

- The overall performance of companies with regard to actions undertaken so far to protect company's processes is generally not perceived to be very good. Suppliers' awareness level and communication regarding security related risks are perceived as poor. The overall supply chain readiness to respond to intentional risks is generally not perceived to be good.
- The meat sector outperforms the vegetable sector in the area of public interface, which includes maintaining records on company's processes and maintaining list of local/national emergency contacts. Process and wholesale/retail stage outperforms the supply stage in maintaining emergency budgets to carry on its operation after occurrence of the risk.
- In the areas of communication management, process management, process technology, metrics and infrastructure management, those companies with past risk experience regarding intentional contamination perform better than those who did not ever face the risk.

Risk perception

Intentional contamination is generally perceived as a threat at company level than at country level and the magnitude of the risk is perceived to be moderate.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS

AEO	Authorized Economic Operators
BRC	British Retail Consortium
CDC	Centers for Disease Control and prevention
FAO	Food and Agriculture Organization
FSIS	Food Safety and Inspection Service
FSS Corp.	Food Safety Specialists corporation
GHP	Good Hygiene Practice
GOARN	Global Outbreak Alert and Response Network
INFOSAN	International Food safety Authorities Network
NFPA	National Food Processors Association
NCFPD	National Center for Food Protection and Defense
SQF	Safe Quality Food
USDA	United States Department of Agriculture
US FDA	United States Food and Drug Administration
WHO	World Health Organization

1. Introduction

1.1 Background

Food is crucial for survival of human beings. As it is very vital for life, it is always highly susceptible to different accidental contaminations and security related risks. It is the most vulnerable to intentional contamination by debilitating or lethal agents (WHO, 2002). Everyone needs to eat, meaning that an attack on food supply has a potential effect to a large portion of the population (Shutske and Kenyon, 2006). Food supply chains begin with a vast number of suppliers and producers (farms) and also include numerous transportation, processing and distribution facilities that are all part of bringing the food to the point of consumption (Coleman, 2004). Food can be intentionally or accidentally contaminated at any time and point along the chain and the occurrence of contamination at one place could have a substantial effect on public health. In addition to the public health impacts, deliberate contamination could cause potentially large economic consequences including costs for response to an attack, disruption of food distribution, trade restrictions, long-term loss of consumer confidence, and ultimately, loss of market-share to a food businesses and the nation[1].

There are different food safety management programs within the food industry such as Good agriculture practice (GAP), Good manufacturing practice (GMP) and Hazard Analysis and Critical Control Point (HACCP) and other HACCP based systems (WHO, 2002). These food safety programs provide manufacturers, wholesalers and retailers the information and tools they need to ensure that they are properly protecting consumers by selling safe and healthy food and operating within the scope of regulatory requirements and best practices. Food safety guidelines and certifications are sometimes considered as food security guidelines. However, according to Takhistov and Bryant (2006), the tools used for food safety are not designed for food security[2]. There are different food security guidelines issued by different organizations such as USDA FSIS and U.S. FDA aimed at preventing the food supply chain from intentional contaminations. Despite these food security guidelines, a US security assessment

[1] Economic consequences of intentional risks will not be investigated in this study
[2] Food security in this study is defined as “protecting the food supply from intentional contamination” not as “peoples physical and economic access to food for life” as defined by WHO (2002).

study identified that areas of communication, management support and interaction with suppliers, customers, and carriers are often overlooked[3].

1.2 Objectives and research questions of the study

As it was previously indicated, the food system is recognized to be the most vulnerable to intentional contamination which could have large effect on public health. The main objectives of the proposed study are:

- To explore companies' activities in preventing the risk of intentional contaminations from occurrence (risk prevention).
- To explore companies' activities in minimizing the size of loss after occurrence (risk mitigation).

In line with the objectives set above, the study includes the following research questions:

- What kind of information do companies share with their suppliers and customers with regard to intentional contaminations?
- What motives/incentives do companies have to share security related information?
- What activities do companies perform to protect from and defend against intentional contaminations?
- What kind of technologies do companies adopt to prevent the intentional contaminations that might arise along the supply chain?
- What activities do companies perform to recover from and stay in operation whenever any security related risks arise along the supply chains?
- How do companies perceive threats to the supply chain security?

1.3 Research framework

Based on a literature review of existing security indicators for supply chains, a conceptual framework for measuring companies' security performance was developed. The conceptual framework has been based on findings from Closs (2005). He identified ten competencies that a company needs to consider to enhance the overall supply chain security.
The competencies are defined as follows:

- Process strategy. Refers to company's philosophy regarding the importance of food supply chain security. This includes different characteristics such as company's senior

[3] NCFPD (2005) annual report: http://www.ncfpd.umn.edu/about/reports/annual_report_2005.pdf

management commitment to security, assigning senior management position and commitment to security; encourage security culture as a necessary condition for implementing an effective security management, considering security as a means to provide competitive advantage, necessary to protect brand and cost of doing business.

- Process management. Refers to how people do things, procedures for dealing with internal operations (shipping, receiving handling etc). This includes characteristics such as employing security guidelines from FSIS, use of test incidents to test supply chain protection capabilities, employing HACCP throughout the supply chain.
- Infrastructure management. Refers to the manner in which a company secures its premises and products. This includes the presence of gates, guards, fences, seals on containers/ trailers and security checks on employees, maintaining empty trailers in secure environment, access control to critical company infrastructure, maintaining restrictive controls, maintaining loaded controls in secure environment and access control for employees.
- Communication management. Refers to training, education and internal communication in food security. This incorporates prevention information and response in food security awareness.
- Management technology. Refers to information technology at the collaboration and company level regarding security. This includes providing valid and timely information to supply chain partners regarding security incident responses.
- Process technology. Refers to diagnostics and tracking systems to monitor processes. This includes uses of RFID technology to track products including salvaged, reworked, and returned products.
- Metrics/measurement. Refers to guidelines regarding how security is measured. This includes implementing industry, company, and government guidelines regarding supply chain security.
- Relationship management. Refers to relationships with suppliers, customers and carriers. This includes use of historical information from security audits to determine if relationships should be maintained with customers and application of specific educational programs for supply chain partners regarding security procedures, incentives for employees, consequences for supply chain partners who fail to comply with security procedures and the use of supply chain security audits for frequently used suppliers.

- Public interface. Refers to relationships with government and public. This includes participation in emergency preparedness planning with appropriate government agencies, collaboration with public health groups, and establishing a risk communications strategy for media/public.
- Service provider management. Refers to relationship with carriers, warehouses, and other service providers. This includes verification of service provider's qualifications, collaboration with service providers to improve security programs and requirement to implement controls that prevent food product contamination from service providers.

After defining the above competencies, he developed a research framework for supply chain security as follows:

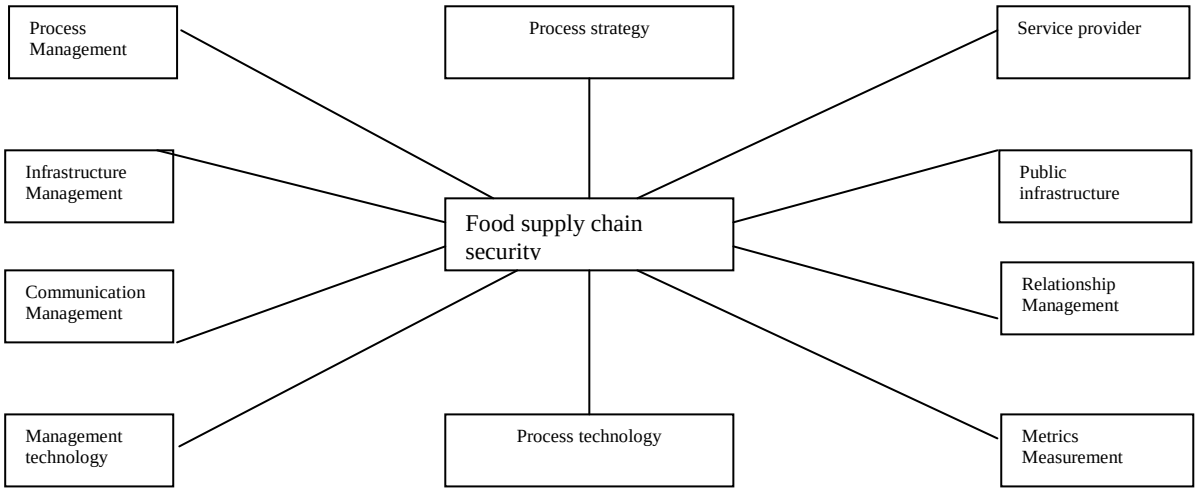

Figure 1: Competency performance drives security and defense performance.
Source: https://www.ift.org/fooddefense/22-Closs.pdf.

The reason in using this framework as a reference to our conceptual framework is that to our knowledge there is no other framework developed to measure security performance in the literature. Therefore, we adopted all the competencies defined above except "service provider management", which has been left out because of its closeness with "relationship management". In our conceptual framework, security performance depends on *risk prevention,* which refers to preventing a risk from occurrence and *risk mitigation,* which refers to minimizing the size of losses after a risk has occurred. Risk prevention includes two main categories: *information sharing* and *control actions* and risk mitigation, or, *robustness,* includes emergency plans and budgets.

The first category, *information sharing*, will address the kind of information (forward and backward) that companies could share with their chain members regarding intentional risks, the motives they have to share such kind of information, the kind of technology they use and the relationship they have with suppliers, customers and government regarding sharing information related to security. *Communication management, management technology, relationship management and public interface* are some of the competencies classified under this category. The second category, *control actions*, will address the activities that companies could perform to protect from and defend against intentional contaminations. Some of these activities include assigning senior management position for security, security control of a company's overall operation (process, premises, etc), control actions which include inspection of suppliers' performance and requesting certifications, employee training and creating awareness among supply chain members and companies participation in different prevention activities with chain partners, government and other stakeholders. *Process strategy, process management, process technology, infrastructure management and security metrics/measurements* are classified under this category. The last variable is *robustness* which refers to the ability of companies to recover and stay in operation. Robustness of a chain is not considered in the previous framework as a separate indicator. In this study, robustness is considered as one aspect that affects the performance of the chain in minimizing losses after occurrence. Robustness includes plans and emergency budgets that companies could maintain to continue their operation. Overall these variables affect the performance of the chain in preventing and minimizing losses of intentional contaminations. Based on the categories mentioned above, the following framework has been developed.

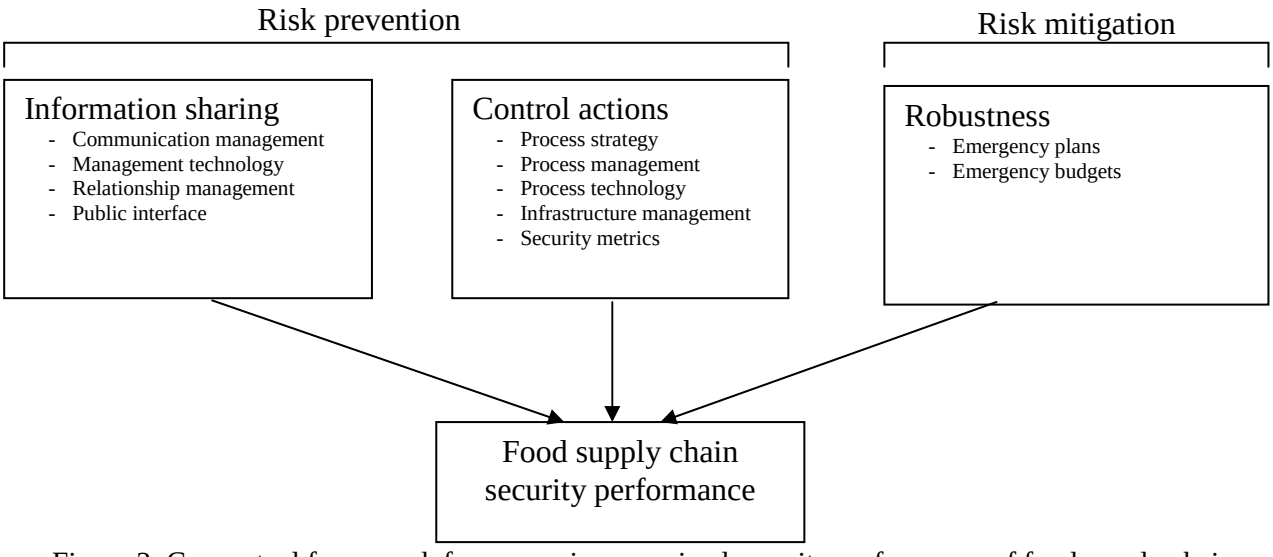

Figure 2: Conceptual framework for measuring perceived security performance of food supply chains.

1.4 Report outline

- Chapter 2 presents the definition and the different certification schemes of food security.
- Chapter 3 presents literature review of food security threats and prevention mechanisms. In this chapter the different types of intentional threats to food supply, ways of preventing the risk, and how companies develop resilient supply chain are discussed.
- Chapter 4 presents the materials used to investigate companies' opinion and attitudes in securing the food supply chain from intentional risks. The sample source and method of analysis used is also presented.
- Chapter 5 presents the findings of the research. Results from the questionnaire are presented and it ends with the particular implications of these findings.
- Chapter 6 contains the conclusion, discussion and suggestions for further research.

2. Defining food security and safety

This chapter will define the concept of food security, food safety and the main difference between the two concepts. In some cases food safety certifications like HACCP are considered as applicable and effective measures to prevent intentional risks to food supply. However, according to (Takhistov and Bryant, 2006), there is a need to update the existing system with the mechanisms to decrease the potential for intentional contaminations of the food supply. So, in this chapter the different certification schemes for supply chain security and the reason why food safety programs like HACCP are ineffective to prevent intentional risks will be presented. The following table shows some of the main points raised in this chapter.

Table 1: Food Security versus food safety.

	Food security	Food safety
Definition	- Safeguarding the food system against intentional contamination.	- Safeguarding the food system against unintentional contamination
Synonyms	- Food defense - Food terrorism	
Similarities	- Prevention of contamination	- Prevention of contamination
Difference	- Concerned with intentional contaminations - Threats often cannot be anticipated	- Concerned with unintentional contaminations - Threats can be reasonably anticipated
Certification schemes	- CARVER+Shock, ISO 28000: 2005, AEO	- HACCP, BRC, SQF, EUREP-GAP, ISO9001:2000, ISO 22000:2005 ,GMP and GHP
Basic principals	- Clearly understand what needs to be protected* - Apply the highest security to the most critical components - Employ a layered approach - Reduce risk to an acceptable level - Security must have strong management support	- Personal hygiene for food professionals[4] - Time and temperature control - Cross-contamination prevention

* http://www.foodsafetyspecialists.com/food_security.htm

2.1 Food security versus food safety

Food security is generally defined as "The process of safeguarding the food system against the intentional contamination. Recently, there has been a change in terminology regarding food security efforts. Several agencies as well as other states and industry organizations are calling food security efforts "*food defense*." This is an appropriate terminology for encompassing all food security efforts. Overall, "food defense" would include all prevention, preparedness, response and recovery efforts (Goodman, 2005). However, the traditional definition of food

[4] http://www.dhhs.nh.gov/DHHS/FOODPROTECTION/LIBRARY/Fact+Sheet/food-safety.htm

security in the world of public health refers to the implication that "all people at all times have both physical and economic access to enough food for an active, healthy life" (WHO, 2002).

According to National Food Processors Association (NFPA) food security is different from food safety in that food security serves as the umbrella under which food safety operates**.** Many businesses are used to think in terms of food safety, and while both food safety and defense are concerned with contamination of the food supply, the food security/defense program helps companies understand how and where food supplies could be intentionally contaminated. Food security threats often cannot be anticipated without intelligence information, and involve criminal acts. Such attacks on the food supply could feasibly occur at any point in food production, and the motivation might include causing illness or death, or producing economic or psychological damage, including consumer fear and loss of confidence in the food supply. In contrast, unintentional contamination of food products can be reasonably anticipated based on the type of food processing involved (Wright, 2007). However, sometimes, though not always, the same precautions can prevent both accidental and intentional disruptions (Suarez, 2006). The US FDA in its progress report "Ensuring the safety and security of the nation's food supply" stated: "Food security and safety are integrated goals. By building upon the nation's core food safety/public health systems and expertise, while strengthening expertise and capabilities needed to address the terrorist threat, FDA is enhancing food security and is improving food safety in the process".

Connecting food safety and food security

Connecting food safety and food security to facilitate the development of a comprehensive food defense strategy should be a major goal (Goodman, 2005). For those who have worked in food safety, the rapidly evolving field of food security is something new and interesting, but may not be fully understood. Effective food safety programs have existed for years, and have been instrumental in ensuring the safety of the food supply. Different programs and connections from food safety efforts can help in developing new food security efforts. Connecting food safety with food security will help to develop new initiatives to raise the awareness of industry and convince companies to become stakeholders in this process and protect themselves against the threat of intentional food contamination. It is imperative that industry, academia, and government enter into a partnership to assess vulnerabilities and make progress over time to secure the food supply (Goodman, 2005).

2.2 Certification schemes on food security and safety

There are different food certification schemes that contribute to safety, quality, and security of the food products and that provide producers, wholesalers and retailers the information and tools they need to ensure that they are properly protecting consumers. HACCP, BRC, SQF, EUREP-GAP, ISO9001:2000, ISO 22000:2005, GMP and GHP are some of the certification schemes issued with regard to safety and quality of food products. The focus of this paper is mainly to the certification schemes related to security of the supply chain. However, all the certifications are not specific to food supply chain; rather they deal with all kinds of supply chains.

CARVER+shock

CARVER+Shock is an offensive targeting prioritization tool adapted from the military version (CARVER) for use in the food industry[5]. The tool can be used to assess the vulnerabilities within a system or infrastructure to an attack. It allows the user to think like an attacker to identify the most attractive targets for an attack. By conducting a CARVER+Shock assessment of a food production facility or process, the user can determine the most vulnerable points in their infrastructure, and focus resources on protecting the most susceptible points in their system. CARVER is an acronym for the following six attributes used to evaluate the attractiveness of a target for attack:

- Criticality - measure of public health and economic impacts of an attack
- Accessibility - ability to physically access a target
- Recuperability - ability of system to recover from an attack
- Vulnerability - ease of accomplishing attack
- Effect - amount of direct loss from an attack as measured by loss in production
- Recognizability - ease of identifying target

A seventh attribute, Shock, has been added to the original six to assess the combined health, economic and psychological impacts of an attack within the food industry. FDA and the Food Safety and Inspection Service (FSIS) of the United States Department of Agriculture (USDA) have used this method to evaluate the potential vulnerabilities of farm-to-table supply chains of various food commodities. The method can also be used to assess the potential vulnerabilities of individual facilities or processes.

[5] http://www.cfsan.fda.gov/~dms/carver.html

ISO/PAS 28000:2005, "Specification for security management systems for the Supply Chain"
ISO/PAS 28000:2005 is a management system specification which has been developed and introduced in response to a demand from the transportation and logistics industry for a common security management standard, with the ultimate objective of improving the overall security of supply chains. The scheme outlines the requirements to enable an organization to establish, implement, maintain and improve a security management system. It is suitable to all sizes and types of organization that are involved in manufacturing, service, storage or transportation at any stage of the production or supply chain that wishes to implement and maintain a security management system[6]. According to ISO press release, its implementation will reassure business partners that security is taken seriously within the organization they deal with.

AEO (Authorized Economic Operators)
AEO is a regulation issued by European commission aiming at increasing security for shipments entering or leaving the EU. This law is enforced since January 2008 across the EU[7]. The introduction of AEO status is the EU's response to the need to secure international supply chains and the introduction of Customs-Trade Partnership Against Terrorism (C_TPAT) in the USA. In the context of EU commission, the concept of AEO should ensure a safer and more secure end-to-end supply chain[8]. Being recognized as an AEO will constitute added value for the operator, as it demonstrates compliance with solid security criteria and controls. And this will provide a competitive advantage to participating companies.

2.2.1 Are food safety measures sufficient for food security?

Food security and HACCP

HACCP is a safety management system that addresses the analysis and control of biological, chemical, and physical hazards existing in the food supply chain. It is designed to identify health hazards and establish strategies to prevent, eliminate, or reduce (to an acceptable level) their occurrence. Corrective actions are necessary if a deviation from the established critical limits occurs during the processing of food stuffs. The HACCP system, in its existing form (www.foodsafety.gov/~fsg/fsghaccp.html), has two major pitfalls that render it ineffective for

[6] http://www.iso.org/iso/pressrelease.htm?refid=Ref981
[7] http://www.logistiek.nl/dossierartikelen/id883-Hoe_werkt_het_AEO_certificeringsproces.html
[8] http://www.cargosecurityinternational.com/channeldetail.asp?cid=14&caid=7868

food security/defense purposes (Takhistov and Bryant, 2006). First, it was not designed to recognize agents such as those associated with intentional contamination, and food processors have not been highly aware of the select agents associated with food terrorism. Second, it lacks standardized corrective actions to resolve post-attack product/facility noncompliance issues. There is a need to update the existing HACCP system - or in some cases, standard operating procedures (SOPs) and/or good manufacturing practices (GMPs)—with the mechanisms to decrease the potential for intentional contamination of the food supply; appropriate systems to ensure early detection of deliberate food contamination at any point along the production pathway, including surveillance and rapid laboratory diagnostic and communication systems; and systems to ensure rapid and thorough response if an intentional contamination is detected, including protection of employees and consumers. Additionally, HACCP fails to address all the necessary components for an initial vulnerability assessment. The process for such an assessment endorsed by FDA, FSIS, the Federal Bureau of Investigation, and the U.S. Dept. of Homeland Security is CARVER+Shock. It differs significantly from HACCP in that it has been modified from its initial use, which was military based, to consider the less-familiar agents associated with an intentional attack; incorporates vulnerability-an element unique to intentionality and dependent on human ingenuity; and includes many other considerations that are not inherent to HACCP (e.g. accessibility, recognizability and shock). The CARVER+Shcok process is an important first step toward identifying system vulnerabilities and assigning priority of available resources to hardening the system. Once conducted, the process should be repeated annually or when significant changes in production warrant reassessment. Vulnerable points may be incorporated into an ongoing HACCP program to enable the updates required to modify an existing HACCP program to address food security/defense concerns (Takhistov and Bryant, 2006).

3. Literature review on food security risks and prevention mechanisms

As it was defined in chapter two, food security in this study deals with safeguarding the food chain from intentional threats. Intentional threats can be introduced by any individual or group of individuals at any time and place along the supply chains. They could use different mechanisms and agents to contaminate the food chain. This chapter first presents a few examples of intentional contaminations occurred at different times and parts of the world. These examples could give an idea on how deliberate contaminations could end up causing death and illness of individuals, who might contaminate the food and above all they could show the occurrence of the risk could be real. Next, this chapter presents the general types of intentional threats to the food supply, the possible risks associated with the different stages of the food chain and how companies and members of the food chain prevent and minimize these intentional contaminations. Moreover, this chapter depicts how companies could develop ways to recover and continue their operation after disruption. Finally, the chapter will conclude with a summary of few scientific researches conducted by different authors to address the issue of food security. Summarizing these studies could help in identifying what has been addressed so far and what needs to be addressed regarding intentional contaminations.

3.1 Food security risks

Purposeful contamination of food can occur at any time and point of the food supply chain from feed to final consumption. There have been many occasions where civilian food supplies have been sabotaged deliberately to frighten or otherwise harm civilian population. For example, according to WHO report 2002, in 1996, a dissatisfied laboratory worker deliberately infected food to be consumed by colleagues with *Shigella dysenteria* Type 2, causing illness in 12 people in the USA. In 1978, in Holland and West Germany 12 children were hospitalized after citrus fruit from Israel was deliberately contaminated with mercury by a Middle East political group. Terrorists stated they were targeting the Israeli economy. In 1984, members of a religious group contaminated salad bars in the USA with *Salmonella typhimurium*, causing 751 cases of salmonellosis. The attack appeared to be a trial run for a more extensive attack intended to disrupt local elections. In 2002, the owner of a fast-food outlet poisoned a competitors breakfast foods with rat poison resulting in 40 deaths and 200

hospitalizations in Banjing, China. Furthermore, in May 2003, a supermarket employee pleaded guilty to intentionally poisoning 200 pounds of ground beef with an insecticide containing nicotine. Although the tainted meat was sold in only one store in the USA, 111 people, including approximately 40 children, were sickened (FDA, 2003). In China in 2001, at least 120 were made ill after eating noodles that had been contaminated by rat poison. The incident was a deliberate attempt by a pair of men to sabotage the noodle factory as part of a business feud[9]. In Canada in 1970, a postgraduate student contaminated his roommates' food with *Ascaris suum* (a parasite); four of the victims became seriously ill. In January 2003, the Centers for Disease Control and Prevention reported that 92 persons became ill after purchasing ground beef from a Michigan supermarket that was intentionally contaminated with nicotine[10].

3.1.1 Intentional threats to food supply chains

There are three general types of intentional threats to the food supply (Coleman, 2004).

A. The use of food or water as a delivery mechanism for pathogens, chemicals, and/or other harmful substances for the purpose of causing human illness or death.
B. The introduction of anti-crop or anti-livestock agents into agricultural systems.
C. The physical disruption of the flow of food/water as a result of the destruction of transportation or other vital infrastructure.

The use of food and water as a delivery mechanism

According to Dahl (2007), the increase in acts of worldwide terrorism has caused food security to become a major concern for the food industry[11]. Deliberate biological or chemical contamination of food or water remains the easiest method for widespread terrorism, according to US CDC and since everyone eats, all are open to an attack. Chemicals, heavy metals like lead and mercury, and living organisms such as bacteria and viruses can all be threats to a safe water supply[12]. These substances can also contaminate food. For instance, individuals/terrorists could release living organisms such as the bacteria that cause tularemia (or rabbit fever-disease that usually occurs in animals and can be transmitted to people through infected insects or animals or by exposure to contaminated water or dust) into the water or food supply. Water can become contaminated at original water source, during treatment, in the pipes that distribute

[9] http://www.ncfpd.umn.edu/docs/GlobalChron.pdf
[10] http://www.gao.gov/new.items/d04259t.pdf
[11] http://www.faqs.org/nutrition/Foo-Hea/Food-Safety.html
[12] http://health.yahoo.com/publichealth-bioterrorism/terrorism-and-other-public-health-threats/healthwise--te7507.html

water and surface water such as rivers. Hazardous chemicals could be deliberately released in liquid or solid form.

The introduction of anti-crop or anti-livestock agents into agricultural systems

Agriculture is a critical national infrastructure. It is a crucial factor in worldwide socio-economic change. Despite the importance of agriculture to economy and well-being of citizens, limited attention has been given to agricultural vulnerability to individual or terrorist attack. There might be different reasons but generally agricultural products are not viewed as susceptible to significant disruption (WHO, 2002). The use of pesticides to control damage of food crops and enhance production has created a controversy related to potential hazards to consumers. While pesticides can be part of a safe food-protection program, they can be hazardous when handled or used as a weapon by terrorists. Biological agents could be targeted directly against humans by using against agricultural crops, feed, livestock, fertilizer, pesticide, herbicide, poultry and fish.

Physical disruption of the flow of food/water as a result of the destruction of transportation or other vital infrastructure

Transportation (airports, ports, subways, highways, rails, postal services and shipping) and other vital human services sectors include a number of sub-sectors, which are complex networks, providing essential goods and services for citizens to survive, such as water, food and agriculture as well as emergency services and public health. The transportation vehicles that hold food in the usual course of business could be used by individuals or terrorists as one way of achieving their targets. The ability to attack the food supply while in transit from the production site is a critical area and possibly the area that has the least amount of protection currently (WHO, 2002).

3.1.2 Stages in the food supply chain and possible risks

A supply chain starts with an enormous number of producers (farms) and numerous transportation, processing and distribution facilities that are all part of bringing the food to the point of consumption. In addition to being susceptible to intentional attacks, this system makes it extremely difficult to trace back and identify the source of the contaminated food (Coleman, 2004).

Agricultural production and processing

Food supply chain starts with suppliers of agricultural inputs to farmers. According to WHO (2002) agriculture production areas can be vulnerable to deliberate contamination, such as with highly toxic pesticides and other chemicals. Certain harvesting practices, such as open-air drying, offer opportunities for deliberate contamination. Irrigation water can also be easily contaminated with chemical or biological agents. The introduction of raw materials into the processing flow is a critical point in processing operations. Thus, sources of raw materials known to be secure should be used whenever possible[13]. The water used in food processing is also important, particularly for minimally processed foods such as fruits and vegetables, where washing is often the critical processing step. Precautions similar to those for drinking-water systems, including the analysis of the water used, should be taken (WHO, 2002). Air systems in processing plants can also be sources of deliberate contamination. In many food-processing systems, heat treatment is also a critical point for microbiological contaminants. From the point of view of deliberate contamination, the normal time and temperature treatments at these control points might not be adequate for all microbiological agents that could be used and would have little or no effect on reducing contamination by toxic chemicals (WHO, 2002). So, individuals or terrorists could create deliberate destruction by introducing biological and chemical agents in primary production and processing steps of the supply chain.

Wholesale and retail distribution

Wholesale and retail distributions are among the most exposed parts of the food supply chain (WHO, 2002). While tamper-resistant and tamper-evident containers have proved to be extremely useful in reducing deliberate contamination, all such containers are vulnerable to individuals who know how to penetrate the protective measures. The storage facilities, transport containers for bulk foods, re-packaging materials could be used as vehicle for deliberate act of contaminating food with different biological and chemical agents. The use of false labels and replaced ingredients which are contaminated with toxic chemicals are also some ways of intentional attacks.

[13] http://www.who.int/csr/delibepidemics/en/annex5.pdf

Food services and restaurants

Food service operations have already been the target of criminal attacks (WHO, 2002). Spice or flavors in open containers in restaurants and institutional settings are vulnerable to deliberate contamination. As it is mentioned in section 3.1, the act of the religious group to contaminate salad bars could be an example to the vulnerability of food service to intentional attack. Automatic giving out equipment, including vending machines, may also be vulnerable to contamination.

Who might contaminate a food product?

Intentional contamination can be introduced by anyone at any time and place along the supply chain. The table below lists some examples of the types of individuals who might be motivated to contaminate food products (FSIS, 2007).

Table 2: Potential internal and external threats to food contamination.

Internal	External
Dissatisfied employee	Organized terrorist
Cleaning crew	Truck drivers (shipping and receiving)
Contractors	Contractors
Temporary employees	Suspect suppliers
Members of terrorist groups posing as employees	Competitors and visitors

Source: Derived from FSIS (2007).[14].

3.2 Risk prevention

As with all health and safety problems, prevention is usually the most desirable option. Prevention is considered first line of defense against intentional contamination[15]. In the context of food terrorism, prevention means preventing the sabotage of food during production, processing, distribution and preparation. According to Shekheta (2006), prevention and response are identified as the two major strategies for countering the threat of food terrorism. The sections below describe the different activities that companies could perform to prevent and minimize the risk of intentional contamination as well as enhance the overall performance of the chain in preventing the risk.

[14] http://www.fsis.usda.gov/PDF/Food_Defense_Plan.pdf
[15] ftp://ftp.fao.org/docrep/fao/meeting/008/j3110e.pdf

3.2.1 Information sharing

Information sharing is a key element in developing comprehensive and practical approaches to defending against potential threats and other attacks (Dacey, 2003). Information on threats, vulnerabilities, and incidents experienced by others can help identify trends, better understand the risks faced, and determine what preventive measures should be implemented. However, establishing the trusted relationships and information sharing protocols necessary to support such coordination can be difficult. The reason for uncertainties in sharing information is that perfect information about the system cannot be secured. While every single member has perfect information about it self, uncertainties arise due to a lack of perfect information about other members. To reduce uncertainties the supply chain member should obtain more information about other members (Yu et al, 2001). Information sharing is important to emergency responders to prepare for and respond to intentional attacks and other emergencies (Dacey, 2003). For example, if a biological attack was to occur it would be important for health officials to quickly and effectively exchange information with relevant experts directly responding to the event in order to respond appropriately.

Success factors for sharing information

Dacey (2001) reported on information sharing practices of organizations that successfully share sensitive or time-critical information. He found the following practices:

- Identifying and agreeing on the types of information to be collected and shared between parties;
- Developing standard terms and reporting thresholds;
- Balancing varying interests and expectations;
- Establishing trust relationships with a wide variety of governmental and nongovernmental entities that may be in a position to provide potentially useful information and advice on vulnerabilities and incidents;
- Developing standards and agreements on how shared information will be used and protected;
- Establishing effective and appropriately secure communications mechanisms; and
- Taking steps to ensure that sensitive information is not inappropriately disseminated.

3.2.2 Communication

Effective communication up and down the food supply chain could also be important to control food hazards. Communication between the company and its suppliers as well as between the company and its immediate customers-helps ensures that all relevant food hazards are identified and are adequately controlled at each step in the supply chain. Communicating with the company's customers and suppliers about known hazards and how to control them also helps to clarify customer and supplier requirements. All parties need to know the feasibility of and need for these requirements, as well as what their impact on the end product might be. Dacey's (2001) study revealed that organizations used a variety of mechanisms to ensure effective and timely communication among members and with the professional and administrative staffs. Regularly scheduled meetings were the primary method of sharing information as well as a method for building trust. These meetings offered a generally secure environment to share information, while also encouraging broader member participation. The study also showed that senior management support for their participation in an information-sharing organization was critical to their success in obtaining valuable information and contributing to the success of the entire information sharing organization. For example, management approval was needed before individuals could share information about potentially sensitive incidents and vulnerabilities. According to FAO/WHO (2004), effective communication among all components of an emergency response system is essential and should be included in preparedness planning. Communication with international components, such as GOARN and INFOSAN for Emergency, should be considered essential in the light of the potential international spread of disease and trade in food. Secure web-based resources can facilitate communication during an emergency response. Working in cooperation with government organizations and the food industry is also in the best position to address threats throughout the food supply system from production to consumption[16]. Government food safety authorities may provide necessary guidance and other coordination functions to assist the industry.

3.2.3 Management and process technology

Management technology refers to the ability to detect potential security threats or incidents, and share timely and reliable information internally and externally. Information systems

[16] ftp://ftp.fao.org/docrep/fao/meeting/008/j3110e.pdf .

provide a first defense mechanism by which to understand trends in product contamination, missing shipments, and the root causes of these occurrences. These information systems also play a critical role in gathering information that is subsequently shared with suppliers, customers, third party service providers, and government agencies to identify potential problems or recovery actions at the intersection between firms (Closs, 2005). Process technology involves the presence, use, and ability of information systems to track the movement of products and monitor processes internally and across the supply chain. Process technologies include the use of tracking technologies, such as Radio Frequency Identification (RFID) and smart-seals, and process improvements. According to Closs (2005) report, most companies have not progressed beyond implementation of physical security measures (for example, gates, guards, and cameras) and have not gained the advantages that may come from tracking technologies. Process technology is one avenue to explore to derive synergistic benefits from security (Closs, 2005). Companies claim that tagging products with RFIDs will facilitate recalls in the event that terrorists poison the food supply. They say the technology can help them to keep precise track of all goods and help in recall efforts should their products be contaminated with poison during a terrorist attack[17].

3.2.4 Operation management and control actions

Operation management refers to security control of a company's overall operation such as physical control which includes routine security checks of the premises for signs of criminal activity or areas that may be vulnerable to such activity. These security checks need to concentrate on sensitive areas (e.g., places where the product is exposed, especially in large batches, in-plant laboratory facilities, water, and computer data). It also includes control of stored materials and chemicals (e.g. cleaning and pest control chemicals, laboratory reagents) on the premises. Such kind of chemicals need to be stored away from food and kept properly labeled. Access to storage areas for these items should be limited to those who need access, based on their job function[18]. Readily available toxic substances could be the contaminant of choice for a dissatisfied employee. Process controls which include assessment of heat treatment, chlorination, washing or other steps that may reduce, remove or destroy a contaminant that has been previously added is also another aspect of operation management. Companies need to make adjustment to these steps and consider in any vulnerability assessment and development of a food security plan.

[17] http://www.wired.com/politics/security/news/2003/08/59624
[18] http://www.fda.gov/ora/training/orau/FoodSecurity/textpages/2.html

Companies control actions include activities such as inspection and control of delivery vehicles, products, packages, unscheduled/after hour deliveries, activities of employees and external parties (e.g. suppliers and other visitors). Delivery vehicles should be properly inspected and secured, especially those carrying bulk fluids[18]. Locked and/or sealed vehicles can discourage in-transit contamination. Attempts to contaminate product can leave detectable signs, such as abnormal powders, liquids, stains or odors, evidence of resealing, or compromised tamper-evident packaging and fake product may show inappropriate or mismatched product identity, labeling, or product coding. Thus, companies should regularly inspect product, packaging, and paperwork at receipt in order to minimize the risk.[19]. Contamination can also occur during offloading, especially after hours because delivering contaminated product may require substitution of part or all of a load, possibly resulting in an error in the type or quantity of product in the load. So, the product type and quantity received should be reconciled at delivery with the product and quantity ordered and listed on the paperwork[19].

With regard to control of employees' activities, management should keep track of who is and should be on duty, and the location in which a person should be working[19]. This can take the form of a shift roster. A dissatisfied employee who has intentionally contaminated product may not return to work. On the other hand, a dissatisfied employee who plans to contaminate product may access areas not normally associated with his/her job function in order to collect intelligence or take other actions in support of the system. So, companies should establish a system of staff identification, such as uniforms or nametags that could allow to easily identify an intruder. Employees' personal items should also be restricted in the facility, especially in sensitive areas[19]. A dissatisfied employee who plans to intentionally contaminate product may need to bring the contaminant into the facility, using personal items, such as a purse, thermos, or lunch bag to disguise it.

3.2.5 Awareness and supervision

One way of preventing risk of intentional contaminations is providing employee's food defense training. The purpose of food defense awareness training is to ensure that employees know their responsibilities. According to FDA (2005), employees should be regularly educated about food defense principles. Specifically, they should be made aware of the vulnerabilities of the company, and the precautions that the management has determined will

[19] http://www.fda.gov/ora/training/orau/FoodSecurity/textpages/2.html

be most effective in preventing an intentional contamination event. Management should make efforts to inform and involve staff in food security. At its core, this means to promote food security awareness on a regular basis. An informed and alert staff is more likely to detect weaknesses in a food security system and to detect and properly respond to signs of intentional contamination. Employees should be encouraged to report suspicious activities, possible product tampering or suspected security system weaknesses to facility management[19]. According to FDA (2005), companies should also communicate and create awareness about the risk of intentional contaminations with their suppliers and other chain members. Suppliers should be encouraged to practice food security. Contamination of raw materials or finished products can occur at a supplier's facility so companies need to consider the use of intra-partner audits and security assessment practices in improving joint security and food defense practice. Companies could also consider making specific security measures part of a supplier's contract.

Appropriate level of staff supervision is also another way of effectively reducing the risk of intentional contaminations. Supervision should extend to cleaning and maintenance staff, as well as new staff[20]. According to FDA (2005) managers should be particularly alert for: unexplained early arrival or late departure; staff accessing information or areas not related to their job function; staff removing documents from the facility; staff asking sensitive questions; or staff bringing a camera to work. Management should screen the background of staff, especially those with access to sensitive areas to reduce the likelihood that someone that is predisposed to illegal activity will be hired or placed in a sensitive position[20].

3.2.6 Risk prevention guidelines

There are some guidance documents on preventive measures for food security that may be used by public health officials or industry in developing some format for assessing vulnerabilities, developing and implementing preventive measures, and educating staff/employees on food security. Some of the guidelines are as follows: FSIS guidelines for processors, FSIS guidelines for meat, poultry, and egg food processors, FSIS guidelines for the transportation and distribution of meat, poultry and egg products, Food safety and food security: what consumers need to know, and FDA’s guidance for industry food producers, processors, and transporters. These guidelines are designed as an aid to food operators (i.e. firms that produce, process, store, repack, re-label, distribute, or transport food or food

[20] http://69.20.19.211/ora/training/orau/FoodSecurity/textpages/1.html

ingredients or that prepare or distribute food at retail) to focus sequentially on each segment of the farm-to-table system that is within their control and to minimize the risk of tampering or criminal or terrorist action at each segment. In this study, FDA's guidance for industry food producers, processors, and transporters is presented. This guidance has different sections that relate to individual components of a food establishment operation: *management of food security* (e.g. assigning responsibility for security to qualified individual(s), investigation of suspicious activities, etc)*; physical security (e.g.* restricting access to sensitive areas, inspecting incoming and outgoing vehicles for suspicious and unusual activity etc.)*; employees* (e.g. pre-hiring screening); *computer systems; raw materials and packaging; operations; and finished products.* It also covers security strategies and evaluation of the security system. For details see Appendix I.

3.3 Risk mitigation

Robustness

In practice robustness and resilience are used interchangeably. However, most researchers used the word resilience instead of robustness. According to Christopher and Peck (2004), a robust process may be desirable, but does not equate itself to a resilient supply chain. So, they defined resilience as "the ability of a system to return to its original state or move to a new, more desirable state after being disturbed". In a corporate world, resilience refers to the ability of a company to bounce back from a large disruption (Sheffi, 2005). This includes, for instance, the speed with which it returns to normal performance levels (production, services, fill rate, etc.). Today's operating environment calls for a supply network design that is both secure and resilient[21]. That means a supply network that has advanced security processes and procedures in place, while at the same time being resilient enough to respond to unexpected disruptions and restore normal supply network operations. Companies need to design for both security and resilience, as a secure supply network does not guarantee a resilient supply network, and vice versa (Rice and Caniato, 2003). Today's operating environment also calls for new organizational plans and capabilities. Specifically, deeper relationships need to be developed with suppliers and customers to co-create a more secure and resilient network[21].

Companies can develop resilience in three main ways: increasing redundancy, building flexibility and changing the corporate culture (Sheffi, 2005).

[21] http://goliath.ecnext.com/coms2/gi_0198-163173/Building-a-secure-and-resilient.html

*Redundancy r*efers to duplicating resources to ensure the availability of a backup solution in case of disruption, or at least spreading the risk. Redundancy can be built increasing inventories, duplicating equipment and facilities, having multiple sources for the same component, etc.

*Flexibility r*efers to the ability to accommodate sudden fluctuations in the availability of resources. In contrast to redundancy, when a company increases supply chain flexibility, it can both withstand significant disruptions and better respond to demand fluctuations. It involves redeploying previously committed capacity.

Corporate culture refers to the creation of a risk management culture in the organization based on clear performance requirements and lines of communication between all supply chain organizations to enhance and make possible supply chain resilience.

Preparedness and response plans

Plans and capabilities developed by businesses and government will facilitate the response and recovery from the negative consequences of either a food safety or food defense event[22]. A food defense plan helps to identify steps that companies can take to minimize the risk that food products in their plant will be intentionally contaminated or tampered with. A plan increases preparedness. Although the plan should be in place at all times, it may be particularly helpful during emergencies[23]. During a crisis, when stress is high and response time is at a premium, a documented set of procedures improves the ability to respond quickly. The effectiveness of a response depends to a great extent on preparedness plans that are developed and implemented long before any event occurs. The components of general preparedness plans that enable and effective emergency response include (WHO, 2002):

- inspection systems to detect public health incidents;
- implementation of preparedness planning principles;
- testing preparedness plans for effectiveness; and
- assessment of vulnerabilities to the specific threat or incident:
    - capacities for investigation and verification of the threat or incident and
    - linkage of the relevant government agencies and other bodies that will contribute to management of the public health consequences.

[22] http://bioterrorism.dhmh.state.md.us/food.htm
[23] http://www.fsis.usda.gov/PDF/Guidance_Document_Warehouses.pdf

3.4 Scientific researches into food supply chain security

In the previous sections we have seen the different types of intentional threats to the food supply and the possible ways of preventing the risk from occurrence and minimizing losses after occurrence. In this section a summary of few scientific researches conducted by different authors in addressing supply chain security issues will be presented. Summarizing these studies could help in identifying what has been addressed so far and what needs to be addressed regarding intentional contaminations. Table 3 presents some of the scientific researches and major findings regarding supply chain security issues. Detailed explanation of the summarized studies is presented in Appendix II.

From the literature studied, it can be concluded that:

- *Food security issues addressed*. Most of the issues addressed are concerned mainly with terrorists' actions. However, as it was shown in Table 2, there are different potential internal (e.g. employees) and external (e.g. organized terrorists) individuals that could deliberately contaminate the food supply.
- *Methods used*. Almost all the studies are conducted using mail and internet survey.
- *Country*. Most of the studies are conducted in U.S. This could be because of the terrorists attack on September 11, where U.S. government organizations, institutions and companies encouraged to protect the nation's food supply. However, as food supply has global movement, the risk of intentional contamination in one country could affect other countries of the world.
- *Time frame*. Most of the studies are conducted after the terrorist attack on U.S.A on 11th September 2001.

Table 3: Scientific researches and findings regarding supply chain security.

Food security issues addressed	**Method used**	**Country**	**Major findings (1)**	**Reference**
Communication on food terrorism	Case study	Netherlands	There is *no international co-ordination*, even though it is known that foods are produced and sold worldwide and, in Europe at least, food problems are often crossborder problems.	(Van Geest, 2002)
Security assessment and benchmarking tool	Mail and internet survey (n= 1400 companies)	USA	<u>Defense practice at retail food and food service, and their wholesale suppliers</u> - *Food service retail* ranks number one as the *most ready* sector followed by food service wholesale, grocery wholesale and grocery retail. - Foodservice wholesale sector outperforms its retail partners by establishing *stronger collaboration* ties with its supply chain partners and devoting more effort to *track and monitor* their food products. - Grocery wholesale sector outperforms the foodservice sector in physical security. - Retailers score lower than manufactures with regard to *readiness for defending* the food system. Manufacturers score lower than foodservice companies. - Intra-company communication and plans are well underway, but *communication* with suppliers or customers is *lacking*. - Firms have generally experienced an *ability to detect incidents* internally and across the supply chain but *not* experienced *ability to decrease incidents.* <u>Transport sector (preliminary results)</u> - Companies are most competent in: *credentialing drivers*, record keeping consistent with FDA bio-security regulation, *inspecting* loaded trailers for tampering, information systems, and *incident response plans*. - Least competent to date in: automated intrusion detection, use of *RFID* for tracking and non-intrusive tracking technology. <u>Manufacturing sectors (preliminary results)</u> Companies that have adopted the most "defense" strategies and practices have done the following: - Have a *senior management* position dedicated to security, *audited security* procedures of contract manufacturers, customers and infrequently used suppliers to determine ongoing relationships, *utilize metrics* to monitor operations, protect brands, and track incidents across the supply chin, *educated supply chain partners* regulatory and have seen performance improvements in detection and resiliency.	(Closs et al, 2006)
Supply chain response to global terrorism: a situation scan	Semi-structured questionnaire and case studies (n=20 companies)	USA	- All respondents are *concerned* with the potential risk related to the consequences of a *terrorist attack* on their supply chain, but there is a general sense of disorientation on how to deal with the problem. - To protect the supply chain from disruption, companies are undertaking a series of initiatives in *physical security*, *information security and freight security.* - To create a *resilient* supply chain, companies highlighted "*company organization*" and "*supply network design*" as the two main areas of intervention.	(Sheffi et al, 2003)

Table 3 (continuation)

Food security issues addressed	Method used	Country	Major findings (1)	Reference
Defending America's food supply against terrorism: Who is responsible? Who should pay	Internet survey (n= 4260 residents)	USA	How should America's anti- terrorism budget be allocated? - *Protecting food* system and protecting against chemical and biological attacks should *receive most funding*. - Spend *more* to protect *food supply* and to defend against chemical/biological attack *than to secure air travel*. - The public is *not confident* that America's food supply is secure. Who is responsible for food defense? - *Governmen*t has primary *responsibility* for food defense. Who should pay for food safety and food defense? - *Government* should bear the *largest portion* of the *costs* of both food safety and food defense. And, government has a larger role in food defense programs than in food safety. - The *same* amount should be spent for food defense as food safety.	(Stinson et al, 2006)

(1) For more explanation about the above summarized issues see Appendix II.

4. Methodology

4.1 Research material

An extensive literature was reviewed to get insight into the concepts raised in this research. There was lack of written materials about the issue of intentional contaminations of food in Europe and the practices and activities that European countries are performing or planning to perform to protect from and defend against any intentional contaminations of the food supply. Thus, most of the theoretical concepts are based on practices from US. Internet journals were the main sources of gathering the literature. In order to collect data a questionnaire was developed with the purpose of investigating a very broad range of issues in line with the questions raised in this research.

4.2 Design of the questionnaire

In order to elicit companies' perceptions about their security performance, a semi-structured questionnaire was designed. The survey consisted of about 100 questions, divided into four parts: (1) *company control actions* which includes questions about the activities (e.g. security control of company overall operation, inspection of suppliers plant, risk awareness programs to employees and supply chain members, companies participation in different prevention activities, etc.), that companies could perform to protect from and defend against intentional contaminations; (2) *company performance* which asks companies to evaluate their own performance in preventing the risk; (3) *information sharing* which includes questions about the kind of information (pre and post risk) that companies could share with their chain members regarding intentional risks, the motives they have to share such kind of information, the kind of technology they use to share security related information, etc.; and (4) *background information* which includes questions about the company's own risk experience during the past five years, companies perception to intentional contaminations, and responsibility and work experience of respondents. A combination of closed and open-ended questions was used. To measure attitude of companies towards the different activities and actions performed to protect from and defend against intentional contaminations, likert scale measurement (ranging from "strongly disagree" to "strongly agree", and an option "not applicable") was used. To evaluate own performance, a five scale rate (ranging from "very poor" to "very good") was used. To get information about the kind of information companies share with their suppliers and customers pre and post intentional risks,

why do they share, and with whom mainly share information about intentional contaminations, open-ended questions were used. The questionnaire was pre-tested by three experts from different food companies in order to test the questionnaire for clarity of the statements and need for additional ideas. The comments and additional ideas given by the experts were incorporated in the final version of the questionnaire (in English). A Dutch cover letter attached with the questionnaire was sent to companies via postal mail addressed specifically to quality managers. Telephone was used for follow up of non-response. The complete questionnaire and cover letter are included in Appendix III.

4.3 Sample

A total of 130 companies participated in the survey. For the purpose of this study, two sectors (meat and vegetable) were selected. The meat sector includes feed companies, processing and wholesale/retail companies. The vegetable sector includes seed companies, processing and wholesale/retail companies. Companies involved have (part of) their business in the Netherlands. Companies and their respective financial status were selected from a database from Agricultural Economics Research Institute (LEI)[24]. The response rate is 18%, i.e. 23 companies returned the questionnaire, including 14 companies from the meat sector (feed and processing), 6 companies from the vegetable sector (seed and processing) and 3 companies from wholesale/retail part. Considering the number of companies invited to participate in this survey, the response rate is relatively low. However, looking at the *average total capital* (for the year 2002-2004) of the *respondents* (Table 4 below), their share out of the *total average capital* of the *companies in the database* in each sector is relatively high, except for vegetable (processing) sector. The results of analysis of the sample (n=23) could give a good indication regarding the security performance of the chain.

Table 4: Respondents share of the total average capital of the sample in each sector.

	Companies in the database	Respondents	*Average total capital of respondents/total average capital of the sample (%).
Feed	31	11	**58
Seed	14	2	23
Pork (processing)	39	3	38
Vegetable (processing)	26	4	9
Wholesale/retail	20	3	17

* Average total capital for the year (2000-2004).
**Financial data for three companies is missing.

[24] The LEI database was derived from Amadeus databank and designed for a study on analyzing the return on equity of four Dutch food supply chains, i.e. dairy, pork, vegetables and fruits. The companies in the database have greater than 4 million average total capital for the period of 2002-2004.

4.4 Method of analysis

Because of the exploratory nature of this study, descriptive statistics such as frequency tables and compare means such as t-test analysis was used. The frequency tables were used to describe issues such as how many of the respondents conduct security practices to their overall operations, perceive intentional contaminations as a threat, prepared to protect from and defend against any intentional contaminations, and share information related to security risks with their employees, suppliers, and customers. Compare means were used to look at whether there is a difference in security practice between the two sectors (meat and vegetable) and between the supply (seed and feed) and process/retail stages of the food supply. Independent sample t-test is used to test whether the difference is significant among the scores of the sectors (meat and vegetable) and stages (supply and processing/retail) of the chain. Data were entered in SPSS for windows version. Open-ended and “other (specify)” responses were coded.

5. Results

5.1 Risk experience and perception

Companies were asked whether intentional risks are threats to own company and to the country in general. At country level, intentional risks are perceived as (very) risky by 10 % of the respondents. 35% regards intentional risks are moderately threatening and 45 % perceives it as not much risk at all. At company level, intentional risks are perceived as real threats by 27% of the respondents, 55% regards as possibly threatening and 18% as not a threat at all. With regard to the risk experience of companies during the last five years, 24% was faced with intentional risks and 23% with recall due to intentional risks. Regarding unintentional risks, 77% was faced with unintentional risk and 62% with recall due to unintentional risks.

5.2 Information sharing

Companies seem not to extensively share information with suppliers and customers. In answering to our question "what kind of information do you share", answers like "*none*", "*what ever necessary*", "*depends on the type of risk*", and "*not applicable*" are some of the responses that were common to all respondents. Answers like "feed safety data sheets", "safeguarding products through certifications", "production process" and "tracking and tracing system" are specified as pre-risk information and "recall procedures'', "tracking and tracing system", "quality assurance and monitoring system", "laboratory results" and "production information" are specified as post-risk information that was shared with suppliers and customers regarding intentional contaminations. Reasons like "protect brand image", "limit liability exposure", and avoid penalties" are identified as company motives to share information regarding intentional risks. In responding to our question "with whom do you mainly share", 31% of the respondents manly share with their suppliers, 16% with government, 15% with customers and 38% with all (i.e., suppliers, government and customers). However, about 80% of the respondents never conduct security meetings with chain partners.

Table 5 shows companies' perceptions about their information sharing practices, subdivided into communication management, management technology, relationship management and public interface management. With regard to communication management, companies do not seem to have established awareness programs for employees and chain members regarding intentional

risks. Regarding management technology results indicate that respondents generally believe that they have implemented an information system that enable them to quickly and consistently share information with their employees and chain partners. Also, more than 60% of the respondents indicate that information on sources and security of products is shared with customers.

With regard to companies' relationship management, companies adopted penalty systems for non-compliance for employees' and suppliers'. However, almost all companies do not have incentive systems. In the field of public interface management, scores show that companies maintain records of product processors and list of local/national emergency contacts. However, in relation to company's involvement with national and international organizations and with government to counteract intentional contaminations, relatively many scores are "neutral". This might indicate that security issues are not well established within the company yet.

Table 5: Perception about own company's information sharing practice in the field of security (n=23).

Our company …	Strongly disagree (%)	Disagree (%)	Neutral (%)	Agree (%)	Strongly agree (%)
Communication management					
Designed awareness programs for chain members	9	46	36	9	-
Established communication procedures for suppliers	9	18	26	36	9
Designed training programs for employees	5	45	32	18	-
Management technology					
Implemented IS[1] that provide timely information	9	14	14	59	4
Implemented IS[1] that provide consistent information	4	9	32	46	9
Impl. IS[1] that quickly share info with all employees	-	-	18	73	9
Impl. a communication strategy for chain partners	9	14	13	59	5
Shares info on sources of products with customers	5	9	18	46	23
Shares info on security of products with customers	-	5	32	46	18
Relationship management					
Adopted incentive systems[2] for chain members	29	52	14	5	-
Adopted consequences for employees' non-compl.	13	9	27	46	5
Adopted penalty system for suppliers' non-compl.	19	19	10	38	14
Public interface management					
Maintains records on company's processes[3]	4	9	4	57	26
Has complete information on suppliers' operations[4]	9	14	36	36	5
Maintains list of local/national emergency contacts	9	13	13	48	17
Works with nat. org. to counteract intentional risks	8	22	39	22	9
Works with internat. org. to counteract intent. risks	24	19	24	24	9
Works with gov. for risk prevention and response	17	4	35	35	9

[1]IS: Information systems.
[2]Such as financial rewards and recognition.
[3]Such as on who is manufacturing, processing, packing, transporting, distributing, receiving, holding products.
[4]On issues such as how they are working, sources of raw materials, with whom they are working.

5.3 Control actions

This section presents the results of analysis regarding control actions that companies could perform to prevent the risk from happening. Most companies regard supply chain security as an objective for securing brand reputation, competitive advantage and market growth. In order to achieve supply chain security, 96% of the respondents operate with HACCP based systems. Also, 60% of the respondents indicate that there are other industry, government or company specific guidelines and requirements to achieve supply chain security. Guidelines like (again) HACCP, Trust Q, GMP+, BRC and IFS are specified as other certification requirements and security guidelines to achieve security of the food supply.

Table 6 shows companies' perceptions about own company's control actions, subdivided into process strategy, process management, process technology, metrics and infrastructure management. Regarding process strategy, about 74% of the respondents assigned responsibility to qualified individuals but do not have senior management position focusing on security. With regard to process management none of the respondents implemented ISO28000:2005. In addition, 57% of the respondents do not conduct inspection on suppliers' operations and plants with regard to intentional risks. However, companies (91%) believe that their suppliers respect hygiene and safety rules. In relation to process technology 81% of the respondents do not use technologies such as RFID and other technologies to verify trailer/container contents, but are able to track and trace products. Regarding infrastructure management, companies seem to work well in restricting access to key facilities and sensitive areas. 82% of the respondents restricted access to key facilities. Companies seem to be better in controlling external parties than internal staff. However, above 50% of the respondents indicate that they provide appropriate supervision to all employees including contract workers, cleaners and data entry staff. Moreover, 68% (not in Table 6) of the respondents evaluates their trust level with employees as good.

Table 6: Perception about own company's control actions in the field of security (n=23).

Our company …	Strongly disagree (%)	Disagree (%)	Neutral (%)	Agree (%)	Strongly agree (%)
Process strategy					
Has a senior management position on security	19	57	5	14	5
Assigned responsibility to qualified individuals	13	9	4	61	13
Process management					
Requests ISO22000:2005 certification from suppliers	26	53	11	5	5
Implemented ISO28000:2005	35	59	6	-	-
Impl. standards to asses suppliers' performance	9	18	23	36	14
Verifies suppliers' background checks on employees	18	50	14	18	-
Uses own audit team to verify procedures in chain	18	23	27	27	5
Use 3rd party audit team to verify procedures in chain	14	27	13	32	14
Inspects suppliers' plants*	39	18	17	26	-
Conducts security tests on suppliers' operations*	35	22	8	35	-
Beliefs suppliers to respect hygiene and safety rules*	5	-	4	68	23
Process technology					
Uses RFID to track products	52	29	14	5	-
Works with suppliers using RFID	50	30	5	10	5
Is able to track and trace products[1]	-	4	4	22	70
Uses technology to verify trailer/container contents	61	28	-	11	-
Has technology to track reworked and returned pr.	17	13	9	48	13
Metrics					
Verifies suppliers' use of security guidelines*	23	23	9	41	5
Infrastructure management					
Conducts security evaluations to determine weaknesses in production processes*	18	9	27	23	23
Conducts security assessments for signs of tamper with products*	30	15	20	10	15
Makes security assessments of the overall operation*	23	9	27	32	9
Evaluates suppliers' overall operation*	26	9	21	22	22
Continuously evaluates logistics system	13	17	39	31	-
Implemented control mechanisms for employees[2]	13	13	30	35	9
Implemented control mech. for external parties[3]	13	13	17	44	13
Restricted access to key facilities (water, control unit)	4	4	9	78	4
Restricted access to sensitive areas (lab, open product)	4	9	18	55	14
Implemented procedures for incoming materials	9	14	23	36	18
Requests locked/sealed containers from suppliers	17	48	13	17	4
Issues identity cards/cloths/badges for employees	9	14	36	32	9
Provides appropriate supervision to all employees[4]	4	13	26	44	13

*Answers were on a liker-scale, i.e. 1 (almost never), 2 (rarely), 3 (sometimes), 4 (usually) and 5 (almost always).
[1]Tracking and tracing of products "one supplier up and one supplier down the supply chain".
[2]Such as background checks, working history and storage of personal items.
[3]Such as badges, permits, uniforms and identification cards.
[4]Including contract workers, data entry, cleaning and maintenance staff.

5.4 Robustness

This section presents the result of analysis to companies' abilities to recover from and continue their operation whenever security related risks occur. Table 7 shows that companies generally seem to be better prepared in case of lack of facilities than in case of lack of raw materials. However, with regard to emergency budgets, only 27% of the respondents agree to have emergency budgets to continue operations in case incident occurs.

Table 7: Perception about own company's robustness in the field of security (n=23).

Our company …	Strongly disagree (%)	Disagree (%)	Neutral (%)	Agree (%)	Strongly agree (%)
Implemented plans for business continuation in case of lack of availability of facilities[1]	4	22	22	48	4
Implemented plans for business continuation in case of lack of availability of raw materials	-	27	22	45	4
Has emergency budgets to continue operations	-	27	41	27	5

[1]Such as electricity, water, transportation, communication and internet.

5.5. Company's own performance evaluation

Companies were asked to evaluate their own and the whole supply chain performance in preventing the risk of intentional contaminations from happening and minimize losses of such risks after occurrence. With respect to relationship with suppliers companies (91%) evaluate their overall work relationship with suppliers' as good and 69% (strongly) agree to be committed to maintain the relationship. Also, 64% of the respondents qualify their trust level with suppliers as good, however; only 39% of the respondents agree to have automatic renewal of delivery contract with suppliers. Regarding companies overall satisfaction, only 38% of the respondents satisfied with suppliers' responsiveness to security and 35% (Table 8) qualify supply chain readiness to respond to intentional risks as poor. Companies (44%) regard the suppliers' awareness level and communication in the field of security related risk as poor. However, 78% (not in Table 8) of the respondents never (rarely) conduct meeting with suppliers regarding security related risks. With respect to own company's security performance, unlike suppliers' responsiveness, Table 8 indicates that 46% of the respondents rate their responsiveness to security risks as good. Regarding to the activities that has been done so far to protect the company process from intentional risks, companies (64%) regard their performance as neutral. Company's performance on securing premises, relationship with suppliers, customers and government with regard to sharing information and overall performance, relatively many scores are below (50%).

Table 8: Perception about company's own and overall chain performance in the field of security (n=23).

How do you rate your company's …	Very poor (%)	Poor (%)	Neutral (%)	Good (%)	Very Good (%)
Performance in securing premises	4	18	30	39	9
Responsiveness	-	13	32	46	9
Activities to protect processes	4	5	64	18	9
Overall performance	4	17	26	44	9
Relationship with suppliers with regard to sharing information	5	30	26	30	9
Relationship with customers with regard to sharing information	-	35	26	30	9
Relationship with government with regard to sharing information	-	22	30	39	9
Suppliers' awareness level and communication	4	44	30	18	4
Supply chain readiness to respond	-	35	35	26	4

5.6. Overall security performance

In the previous sections (sections 5.1- section 5.5), we have seen companies perception for each security performance measuring variable. This section presents the overall performance scores of the competences under each category (i.e. information sharing, control actions and robustness) of the conceptual framework, the relationship between the categories of the conceptual framework and the overall perceived security performance score. This section also presents the comparison between the two sectors (meat and vegetable) and stages (supply and process/retail) of the food supply chain with regard to the perceived security performance score. Moreover, this section presents companies performance scores considering past risk experience and total average capital.

5.6.1 Performance scores of the competencies in each category of the conceptual framework

In order to compare the overall mean scores of the competencies, following the definitions of Closs (2005) presented in section 1.3, all the variables in the questionnaire are grouped into the competencies presented under each category of the conceptual framework. To check whether these grouped variables are internally consistent, a reliability analysis (Cronbach's alpha) has been performed. Accordingly, communication management scores (0.780), management technology (0.749), relationship management (0.695), public interface management (0.831), process strategy (0.619), process management (0.905), process technology (0.644), infrastructure management (0.887), robustness (0.226), company's own performance (0.878). Cronbach's alpha will generally increase when the correlations between the items increase and the commonly-accepted rule of thumb is that α of 0.6-0.7 indicates lower acceptable reliability (Hair et al., 2006). Accordingly, except robustness, all the variables that are grouped under each competency are internally consistent, i.e. the grouped variables under each competency can measure the same aspect. Robustness scores lowest; this might be because of the number of items included in the scale. According to Field (2005), the smaller the number of items on the scale, the lower the value of α will be. Thus, to avoid this problem the three variables that are classified under robustness are considered separately.

Comparisons of the overall mean scores of the competencies in each category

In order to identify the competency in which companies perform well within each category, a comparison between the overall mean scores of each competency has been performed. Moreover,

to test the significance difference between the competencies, paired sample t-test has been done. Accordingly, Table 9 shows the following results:

Information sharing. In this category, management technology significantly (p-value < 0.1) outperforms all the other competencies while communication management gets the least score. Table 9 also shows that the mean ratings of communication management and relationship management belong to the same group (indicated as "a") because they do not have significant differences. All other mean pairs of security performance competence are significantly different from each other at 90% degree of confidence.

Control actions. In this category, infrastructure management (e.g. restricting access to key facilities and sensitive areas) out performs all the other competencies while metrics gets the least score. All pairs having similar alphabets as superscripts as shown in the table below have non-significant mean differences and, thus, belong to the same group. There are three groups of security performance competencies that have significantly different mean ratings though. They are process strategy and process management (p-value = 0.084), process management and infrastructure management (p-value = 0.001) and process technology and infrastructure management (p-value =0.073) significant at 90% degree of confidence.

Robustness. In this category, emergency budgets get the least rating while plans in case of lack of raw material get the best rating. However, all the variables have insignificant mean differences and so belong to the same group (indicated in the Table 9 as "a").

Table 9: Cross-comparison of the overall mean scores of the competencies by category.

	Overall Mean (n=23)[1]
Information sharing	
Communication management	2.64 [a]
Relationship management	2.64 [a]
Public interface management	3.26
Management technology	3.59
Control actions	
Metrics	2.70 [abf]
Process management	2.77 [ac]
Process technology	2.86 [cbd]
Process strategy	3.00 [def]
Infrastructure management	3.16 [e]
Robustness	
Emergency budgets to continue operations	3.09 [a]
Continuation plans in case of lack of facilities	3.26 [a]
Continuation plans in case of lack of raw materials	3.27 [a]

[1]Superscript characters indicate non-significant difference at 90% degree of confidence.

5.6.2 Relationship between the categories of the conceptual framework

To test the relationship between the categories (information sharing, control actions, plans in case of lack of facility, plans in case of lack of raw materials and emergency budgets) a correlation analysis has been performed. Accordingly, results reveled that all the categories have positive correlation with each other which is significant at 90% degree of confidence. This indicates the variables are consistent in measuring the perceived security performance. Moreover, a correlation analysis was performed in order to compare company's own performance evaluation scores with the overall perceived security performance results derived from the three categories (information sharing, control action and robustness) of the conceptual framework. The hypothesis was the results of analysis of these categories should be comparable to the companies own performance evaluation. Results reveled that companies perceived security performance is highly correlated with their own performance evaluation results with a correlation coefficient of (r) = .813 which is significant, at p-value < 0.1 indicating that our evaluation to the companies performance regarding security is highly comparable with their own security performance evaluation, which makes our analysis valid.

5.6.3 Comparison of the performance scores of the meat and vegetable sectors

To compare the performance scores of the two sectors (meat and vegetable), independent sample t-test has been performed. Accordingly, looking at the p-values of the meat and vegetable sectors (Table 10), public interface (p-value = .094) shows significant difference at 90% degree of confidence indicating the meat sector outperforms the vegetable sector in activities such as maintaining records on company's processes, maintaining information about supplier's operation and working with national and international organizations. All the other competencies do not show a significant difference between the sectors.

5.6.4 Comparison of the performance scores of the supply and process/retail stages

As it can be seen from Table 10, comparing the mean scores of the two stages (supply and process/retail); all the competencies do not show significant difference in performance except *emergency budgets to continue operation*. Looking at the p-values of the sectors, *emergency budgets to continue operation* show significance difference at 90% degree of confidence with (p-value = 0.065) indicating the process/retail stage gives more attention in maintaining emergency budgets to continue operation than the supply stage. This indicates the closer the stages of the

food chain towards consumers the higher their concern to maintain emergency budgets in order to minimize the loss after occurrence.

Table 10: Mean scores of the two sectors (meat and vegetable) and stages (supply and process/retail) of the food supply chain.

	Overall mean (n=23)	Sectors			Stages of the chain		
		Meat[1] (n=14)	Vegetable[2] (n=6)	P-value (90%)	Supply[3] (n=13)	Process /retail[4] (n=10)	P-value (90%)
*Information sharing**							
Communication management	2.64	2.79	2.27	0.103	2.62	2.96	0.160
Management technology	3.59	3.68	3.36	0.153	3.54	3.64	0.362
Relationship management	2.64	2.86	2.53	0.288	2.56	3.04	0.149
Public interface management	3.26	3.36	2.85	0.094	3.18	3.37	0.299
*Control actions**							
Process strategy	3.00	3.04	2.67	0.259	2.85	3.20	0.224
Process management	2.77	2.86	2.41	0.131	2.83	2.69	0.348
Process technology	2.86	2.83	2.77	0.442	2.71	3.05	0.175
Metrics	2.70	2.86	2.40	0.248	3.00	2.56	0.228
Infrastructure management	3.16	3.05	3.22	0.324	3.08	3.26	0.310
*Robustness**							
Continuation plans in case of lack of facilities	3.26	3.14	3.33	0.361	3.15	3.40	0.287
Continuation plans in case of lack of raw materials	3.27	3.15	3.33	0.360	3.17	3.40	0.286
Emergency budgets to continue operations	3.09	3.15	3.17	0.488	2.83	3.40	0.065
*Company's own performance evaluation***	3.18	3.21	2.98	0.258	3.21	3.14	0.411

* Answers were on a likert scale, i.e. 1 (strongly disagree), 2 (disagree), 3 (neutral), 4 (agree), 5 (strongly agree).
** Answers were on a likert scale, i.e. 1 (very poor), 2 (poor), 3 (neutral), 4 (good), 5 (very good).
[1] Meat sector includes feed companies and processors.
[2] Vegetable sector includes seed companies and processors.
[3] Supply stage includes feed and seed companies.
[4] Process stage includes processors and wholesale/retail companies.

5.6.5 Companies performance scores considering past risk experience

In Table 10 we have not seen a significance difference between the sectors (meat and vegetable) and stages (supply and process/retail) of the food supply chain with most of the risk prevention and risk mitigation competencies. In searching for other variables that might affect company's security performance, we consider companies *past risk experience with regard to intentional risks and total average capital.* By considering companies past risk experience with regard to intentional risks, the hypothesis was that those companies who faced the risk in the past could perform well in securing their company and the food supply in general. Table 11 shows, the perceived performance scores of companies' who faced/not faced the risk of intentional contaminations classified into (Yes, No) options. To check whether there is a significance difference between the mean scores of the competencies, independent sample t-test was used.

Looking at the p-values of companies past experience related to intentional contaminations, we see a significant difference in performance scores between those companies who faced intentional contaminations and did not face the risk during the past five years. Five of the

competencies: *communication management*, which includes designing of awareness programs and communication procedures to employees and chain partners; *process management*- which includes among others security tests of suppliers' operation and request of certification; *process technology*, which includes implementation of technologies such as RFID; *metrics*, which refers to verification of suppliers' use of security guidelines; and *infrastructure management*, which includes among others continuous security assessment of production process, restriction of sensitive areas and implementation of control mechanisms to employees and to external parties and show significant difference at 90% degree of confidence. Company's own performance evaluation also shows significant difference. This could be interpreted as companies who faced the risk in the past might learn a lesson from it and give more attention to security comparing to those who did not ever face the risk. However, unlike the other variables e*mergency budgets to continue operations* show lower score with companies who have past risk experience indicating those companies who did not face the risk in the past maintain emergency budgets than those who have past risk experience. This seems strange but it could be interpreted as those who faced the risk might know how to handle the risk and how much to maintain for emergency than those companies who did not ever face the risk.

5.6.6 Companies performance scores considering total average capital

As it was mentioned in section 5.6.5, *companies' total average capital* was the other variable that was considered to influence company's security performance. By considering this variable the hypothesis was those who are largest companies in terms of their capital most likely have more financial resources to invest in security and hence enhance their security performance. As it can be seen from Table 11, the comparison is made between those companies' who have below and above 500 million Euros of total average capital. Independent sample t-test is used to check whether there is a significance difference between the mean scores of these factors.

Comparing the mean scores of companies having less than 500 million Euro with companies having greater than 500 million Euro total average capital, there is a significant different in the field of *management technology* and *public interface management* at 90% degree of confidence. This indicates companies having a total average capital less than 500 million Euros generally seem to be better of in *management technology*, which includes among others implementation of information technology and *public interface*, which includes maintaining of company process records and work with national and international companies. In this case it is difficult to say that

the size of company's total average capital has influence over the overall security performance. This is somehow similar with the findings of Kinsey et al. (2007).

Table 11: Perceived performance scores considering companies past experience regarding intentional contamination and total average capital.

	Overall mean (n=23)	Past experience related to intentional contaminations			Total average capital		
		Yes (n=6)	NO (n=17)	P-value (90%)	<500 million (n=17)	>500 million (n=3)	P-Value (90%)
*Information sharing**							
Communication management	2.64	3.28	2.41	0.027	2.67	2.56	0.428
Management technology	3.59	3.81	3.51	0.173	3.62	2.94	0.029
Relationship management	2.64	3.11	2.47	0.236	2.76	2.00	0.152
Public interface management	3.26	3.61	3.14	0.121	3.34	2.72	0.097
*Control actions**							
Process strategy	3.00	3.42	2.85	0.140	3.08	2.50	0.171
Process management	2.77	3.56	2.50	0.001	2.84	2.29	0.123
Process technology	2.86	3.61	2.59	0.004	2.85	3.00	0.385
Metrics	2.70	3.67	2.50	0.033	2.87	2.33	0.264
Infrastructure management	3.16	3.64	2.99	0.045	3.25	2.87	0.209
Robustness							
Continuation plans in case of lack of facilities	3.26	3.50	3.18	0.256	3.41	3.67	0.329
Continuation plans in case of lack of raw materials	3.27	3.17	3.31	0.377	3.12	3.67	0.185
Emergency budgets to continue operations	3.09	2.67	3.25	0.087	3.12	3.00	0.422
*Company's own performance evaluation***	3.18	3.54	3.06	0.080	3.12	2.81	0.166

* Answers were on a likert scale, i.e. 1 (strongly disagree), 2 (disagree), 3 (neutral), 4 (agree), 5 (strongly agree).
** Answers were on a likert scale, i.e. 1 (very poor), 2 (poor), 3 (neutral), 4 (good), 5 (very good).

6. Conclusion and discussion

This final chapter presents the main conclusions, discussions and suggestions for further research.

6.1 Main conclusions

Based on the results of the 23 respondents representing the meat and vegetable supply chains, the following main conclusions are drawn with regard to the three categories (information sharing, control actions, and robustness) which are categorized under *risk prevention* and *risk mitigation.*

Conceptual framework

The risk prevention and mitigation categories of the conceptual framework show positive correlation with each other indicating that these variables are consistent with each other and measure the same thing (security performance). The variables also have positive correlation with the companies' own performance evaluation scores. This indicates that there is no discrepancy between what was measured using these variables and how the companies rated themselves. All in all, though we could not test (because of the smaller sample size) whether the variables are explanatory to the perceived security performance or not, we can say that the variables which we use to measure security performance have fairly high consistency and that the conceptual framework we built is reliable. This does not, however, mean that there are no other alternative indicators which might prove as reliable, and even better.

Risk prevention

- Companies hardly share information with suppliers and customers regarding intentional contaminations. Information sharing practices that are more closely related to food safety assurance, such as implementing information systems, maintaining records on company's production processes, sharing sources of products, tracking and tracing, and recall procedures are well undertaken.
- The main motives of companies to share security related information with chain partners and consumers are specified as limiting liability exposure, avoiding penalties and protection of brand image.
- With regard to control actions findings are somewhat similar as for the information sharing practices: control actions that have close relationship with food safety issues such

as assigning responsibility to qualified individuals and restricting access to key facilities and sensitive areas are well undertaken. Security related practices, such as assigning senior management position focusing on security, use of RFID and other technologies to verify container contents, inspecting suppliers' plants are not well undertaken.

- HACCP is considered as the main guideline and certification scheme to prevent intentional contaminations. Security specific certifications such as ISO28000:2005 and guidelines issued by FDA and USDA FSIS are not implemented.

Risk mitigation

- Robustness seems to better organized at company level (i.e. when there is a lack of facilities) than at supply chain level (i.e. at times of lack of raw material).With regard to emergency budget companies do not seem to agree to maintain emergency budgets to carry on operations after occurrence of the risk.

Performance

- The overall performance of companies with regard to actions undertaken so far to protect company's processes is generally not perceived to be very good.
- Suppliers' awareness level and communication regarding security related risks are perceived as poor. The overall supply chain readiness to respond to intentional risks is generally not perceived to be good.
- The meat sector outperforms the vegetable sector in the area of public interface, which includes maintaining records on company's processes and maintaining list of local/national emergency contacts. This finding excludes wholesale and retail chain partners.
- Process and wholesale/retail stage outperforms the supply stage in maintaining emergency budgets to carry on its operation after occurrence of the risk.
- In the areas of communication management, process management, process technology, metrics and infrastructure management, those companies with past risk experience regarding intentional contamination perform better than those who did not ever face the risk. Generally, control actions are well exercised by those who have past risk experience.
- Size of companies in terms of capital does not seem to affect companies' security performance.
- Intentional contamination is generally perceived as a threat at company level than at country level and the magnitude of the risk is perceived to be moderate.

6.2 Discussion

6.2.1 Reflection with the literature

According to Dahl (2007), the increase in acts of worldwide terrorism has caused food security to become a major concern for the food industry. However, in our case food security does not seem to be a major concern. For some companies food security seems a new issue or may not be fully understood. There is a mixing of food safety and food security practices. Most companies seem to think that they have carried out food security practices considering the food safety practices in place. For example, food safety certification schemes such as HACCP are considered as the main guideline and certification scheme to measure and prevent intentional risks to the food supply; however, according to Takhistov and Bryant (2006) HACCP is not designed to be used for food security purpose. There are other security specific certification schemes such as CARVER+shock and ISO28000:2005, which are not well recognized in our case. In this regard, there seem to be gab in creating awareness regarding food security issues. According FDA (2005), one way of preventing risk of intentional contamination is providing food defense training to employees and chain members. If employees are not well aware of what security risk mean, it is difficult to detect whether the risk is intentional or not, as the result prevention and control of the risk could be difficult. However, companies do not seem to give more attention to this area. Our study revealed that they hardly share information pre and post occurrence of the risk with suppliers and other chain partners. This finding is in line with the findings of Closs et al. (2006). However, according to Decey (2003), sharing incidents experienced by others can help to identify trends, better understand the risks faced and determine what preventive measures should be implemented.

Awareness regarding food security issues could also enhance companies ability to exercise the control actions within own company operations and external activities (e.g. suppliers risk prevention activities). In this regard, control actions seem to be exercised more in controlling company's own internal activities such as controlling access to facilities and sensitive areas than external activities such as inspecting supplier's plant in preventing the risk of intentional contaminations. However, according to FDA (2005) contamination of raw materials or finished products can occur at supplier's facility. Suppliers feel that they are less vulnerable to intentional contaminations. However, according to WHO (2002), individuals or terrorists could use materials such as pesticides, fertilizers, animal feeding substances and irrigation water to intentionally

contaminate the food supply. In this case intra-partner security assessment seems to be important in preventing intentional risks to the food supply. Implementing food security guidelines (for instance FSIS (2003), and FDA (2007))[25], which are not well applied in our case, might also be helpful in guiding which activities of suppliers or other chain partners need assessment and control in preventing the risk.

Though the risk of intentional contamination is not generally perceived to be threatening at country as well as at company level, due to the global movement of the food supply and the difficulty of anticipating intentional risks (i.e. what kind of intentional risk, when and by whom could be introduced), companies need to maintain plans and emergency budgets in order to facilitate minimization and recovery from incidents. Dacey (2001) stated that senior management participation, which is not well undertaken in our case, is important for the implementation of the plans and emergency budgets. In addition to maintaining emergency plans and budgets, cooperative work with national and international organization and with government could also be important to prevent and minimize the risk. However, this practice does not seem well understood. This might lead to the conclusion drawn by Van Geest (2002): "there is no international co-ordination, even though it is known that foods are produced and sold worldwide and, in Europe at least, food problems are often crossborder problems". According to WHO (2002), though the primary means for minimizing risks lie with the companies in the food industry, cooperative work with supplier, customers, and government organizations generally facilitate prevention and minimization of losses.

6.2.2 Methods and materials

Framework for measuring perceived security performance

The selection of the perceived security performance measuring categories (i.e. information sharing, control actions, and robustness) of the conceptual framework has been done based on review of literature on security related issues. The risk prevention competencies for measuring each category of the conceptual framework have been selected from the works of Closs (2005). As it was mentioned in section 1.3, the reason in using his framework as a reference was that to our knowledge no other security measurement framework existed in the literature. He identified ten competencies: communication management, management technology, relationship

[25] http://www.fsis.usda.gov/oa/topics/transportguide.pdf
http://www.cfsan.fda.gov/~dms/secguid6.html

management, public interface, process strategy, process management, process technology, metrics, infrastructure management and service provider management. As we have pointed out in section 1.3, the later has been left out due to its closeness with relationship management. The competencies were classified under each category of the conceptual framework based on the definitions from the literature. Though the competencies were important and inclusive in measuring the perceived security performance of the members of the food supply, did not seem readily understandable, i.e. the competencies need translation into more familiar and understandable terms of the food system. Recently, Kinsey et al. (2007) developed a framework for measuring security performance by rearranging and re-labeling the ten competencies identified by Closs (2005) into operational practices within the food system. This publication appeared later than the conceptual framework used in. However, the perceived performance measuring variables used in our study are in line with both Closs (2005) and Kinsey et al. (2007) publications.

Materials

The database we used in this research was obtained from Agricultural Economic Research Institute (LEI). The LEI database was derived from Amadeus databank and designed for a study on return on equity of four Dutch food supply chains, i.e. dairy, pork, vegetables and fruits. In this study, observations were selected from the database based on the criteria of having greater than 4 million total average capital for the period of 2002-2004. In this study company's current financial status was not taken into account because of the unavailability of recent data. Though the size of companies in terms of average total capital, as it was mentioned in subsection 5.6.6, does not show a significant difference in the security performance; considering their current financial status might change the results by considering some financial measuring variables.

In addressing the objectives raised in this study, a semi-structured questionnaire was used. As it was mentioned in section 3.4, most studies conducted in this field of study were conducted based on mail and internet surveys. The questionnaire was sent to 130 companies from meat and vegetable sectors and their respective chain partners (seed, feed, processing and wholesale/retail). However, as is usually the case for other researchers like Kinsey et al. (2007); the response rate to our questionnaire was relatively low. Consequently, we analyzed the results based on the 23 respondents which as the result made difficult to generalize the perceived security performance of the food supply chain. Therefore, the results of this study are interpreted to the sample (n=23). There might be reasons for the low participation of companies in the surveys. The first reason

could be because of confidentiality concerns, although the names of the participating companies and any confidential information are not disclosed. Another possible reason could be lack of awareness of the issue raised in the questionnaire. Lastly, since our questionnaire was directed to specific quality/safety mangers, they might not have enough time to fill the questionnaire. Therefore, further study is needed to assess what specific security performance activities could companies implement to prevent the risk using web-based survey systems and case studies.

6.3 Suggestions for further research

The susceptibility of the food chain to security related risks is well recognized in the post 9/11 terrorists attack in the US, where companies have been encouraged to adopt new measures to protect the food supplies. Then after, attention is given by individual researchers and universities to address the vulnerability of the food system for security related risks. In this regard, our study could only give some indication on how companies perceived the risk, their awareness level and how they are dealing with it. Thus, to have a broad view of the perception and reaction of companies towards food security, it is advisable to consider future works that incorporate the following points:

- In this study we have examined the perceived security performance of the meat (pork chain) and vegetable sectors and their respective chain partners (seed, feed, processing and wholesale/retail) of the food supply chain. However, it is difficult to generalize the results to the whole food supply chain. Therefore, it would be interesting to extend the assessment to all the sectors in the food supply chain and examine the security performance of each sector and member of the food chain. Furthermore, it would also be interesting to assess the perception of consumers towards food security related risks.
- In addition to survey, it would also be advisable to consider conducting case studies in order to get insight on what specific activities (i.e. activities that are not related to safety) do companies perform to manage security related risks.
- The aim of this research was to assess companies' activities in preventing and minimizing the risk of intentional contaminations. Economic consequences of the risk were not assessed in this study. So, it would be interesting to conduct further research to assess the economic consequences of intentional contaminations to the food industry and to the nation in general and asses the effect of implementing security related programs and practices on the financial performance of the companies and chain partners in the food supply chain.

References

Christopher, M. and H. Peck (2004). "Building the resilient supply chain." International Journal of logistics management **15**: 4-29.

Closs, D. (2005). "Dimensioning a secure supply chain." Proceedings of the institute of food technologists' first annual food protection & defense research conference.

Closs, D., A. Erera and J. Kinsey (2006). "Terrorism, pandemics, and natural disasters: food supply chain, preparedness, response, and recovery". In: Symposium summary, University of Minnesota. http://foodindustrycenter.umn.edu/vd/Events/disasterresponsesummary.pdf.

Coleman, K. (2004). "Bioterrorism and the food supply." Directions Magazine. http://www.directionsmag.com/article.php?article_id=667&trv=1.

Dacey, R. F. (2001). "Information sharing: Practices that can benefit critical Infrastructure." United States General Accounting Office (GAO).

Dacey, R. F. (2003). "Information sharing responsibilities, challenges, and key management issues." United States General Accounting Office (GAO).

FAO/WHO (2004). "Prevention and Response to intentional contamination." Second FAO/WHO global forum of food safety regulations (Agenda Item 5.4 Bangkok, Thailand).

Field, A. (2005). "Discovering Statistics using SPSS." **2nd edition**.

Goodman, T. (2005). "Connecting food safety and food security." Journal of the association of food and drug officials **69**: 6-10.

Hair, J., W. Black, B. Babin, R. Anderson and R. Tatham (2006). "Multivariate data analysis." **6th edition**.

Kinsey, J., K. Kaynts and K. Ghosh (2007) "Defending the food supply chain: Retail food, food service and their wholesale suppliers." University of Minnesota.

Rice, J. B. and F. Caniato (2003). "Building a secure and resilient supply network." Supply chain management review: 22.

Sheffi, Y. (2005). "Supply chain strategy: Building a resilient supply chain." A newsletter from Harvard business school and the MIT center for transportation and logistics **1**.

Sheffi, Y., J. Rice, J. Fleck and F. Caniato (2003). "Supply chain response to global terrorism: A situation scan."http://web.mit.edu/scresponse/repository/euroma_paper_041603.doc.

Shekheta, M. A. F. (2006). "Terrorist threats to food and water supplies and the role of HACCP: Implementation as one of the major effective and preventive measures." Journal of Food safety **18**: 30-34.

Stinson, T., J. Kinsey, D. Degeneffe and K. Ghoshl (2006). "How should America's anti-terrorism budget be allocated?" In: Research report to National Center for Food Protection and Defense, University of Minnesota.

Shutske, J. M. and S. Kenyon (2006). "Why would Agriculture be a target?" Extension Disaster Education Network (EDEN) (Agro-security; Background information).

Suarez, E. M. (2006). "Food safety and supply chain security: The new regulation of international trade ". Williams Mullen International Trade & Customs Report May 2006.

Takhistov, P. and C. M. Bryant (2006). "Protecting the food supply." International Food safety & Quality Network- discussion forum (Food Technology): 34-43.

Van Geest, I. (2002). "Communicating food terrorism." http://www.fsis.usda.gov/Orlando2002/presentations/ivangeest/ivangeest_text.htm

World Health Organization (2002) "Terrorist threats to food: guidance for establishing and strengthening prevention and response systems." http://www.who.int/foodsafety/publications/general/en/terrorist.pdf

Wright, C. (2007). "Food defense." Center for Industrial Services (CIS); *Institute* for public service - University of Tennessee (Safety Compliance & Assistance).

YU, Z., H. Yan and E. Cheng (2001). "Benefits of information sharing with supply chain partners." The Hong Kong Polytechnic University, Kowloon, Hong Kong.

Websites:

FDA (2003). Guidance for industry food producers, processors, and transporters: food security preventive measures guidance http://www.cfsan.fda.gov/~dms/secguid6.html.

FDA (2005). An introduction to food security awareness http://www.fda.gov/ora/training/orau/FoodSecurity/startpage.html.

FDA (2007). Food defense and terrorism: CARVER + Shock software tool. http://www.cfsan.fda.gov/~dms/carver.html.

FSIS (2002). Security guidelines for meat, poultry, and egg food processors. http://www.agrosecurity.uga.edu/annexes/Annex23_Processors.pdf.

FSIS (2002). Security guidelines for food processors. http://www.fsis.usda.gov/OA/topics/SecurityGuide.pdf.

FSIS (2003). Safety and security guidelines for the transportation and distribution of meat, poultry and egg products. http://www.fsis.usda.gov/oa/topics/transportguide.pdf

FSIS (2007). Developing a food defense plan for meat and poultry slaughter and processing plants. http://www.fsis.usda.gov/PDF/Food_Defense_Plan.pdf

Appendix I U.S. FDA guidance for industry food producers, processors, and transporters: food security preventive measures guidance

Management of food security

Security procedures

- Assigning responsibility for security to qualified individual(s).
- Encouraging all staff to be alert to any signs of tampering with product or equipment, other unusual situations, or areas that may be vulnerable to tampering, and alerting identified management about any findings(e.g., providing training, instituting a system of rewards, building into job performance standards).

Investigation of suspicious activity

- Immediately investigating all information about suspicious activity
- Alerting local law enforcement about all suspected criminal activity

Supervision

- Providing an appropriate level of supervision to all employees, including cleaning and maintenance staff, contract workers, data entry and computer support staff, and especially new employees.
- Conducting daily security checks of the premises for signs of tampering with product or equipment, other unusual situations, or areas that may be vulnerable to tampering

Mail/packages

- Implementing procedures to ensure the security of incoming mail and packages(e.g., securing mailroom, visual or x-ray mail/package screening)

Physical facility

Visitors

- Inspecting incoming and outgoing vehicles for suspicious, inappropriate or unusual items or activity.
- Restricting entry to the establishment (e.g., checking in and out at security or reception, requiring proof of identity, issuing visitors badges-collected upon departure)
- Ensuring that there is a valid reason for the visit before providing access to the facility-beware of unsolicited visitors.
- Restricting access to food handling and storage areas (e.g., accompanying visitors, unless they are otherwise specifically authorized).
- Restricting access to locker rooms.
- Apply the above procedures to everyone, including contractors, supplier representatives, truck drivers, customers, couriers, third-party auditors, regulators, reporters, visitors, etc.

Physical security

- Protecting perimeter access with fencing or other appropriate deterrent.
- Securing doors (including freight loading doors), windows, roof openings/hatches, vent openings, trailer bodies, tanker trucks, railcars, and bulk storage tanks for liquids, solids, and compressed gases, to the extent possible.
- Minimizing the number of entrances to restricted areas.
- Minimizing places that could be used to hide temporarily intentional contaminants (e.g., minimizing nooks and crannies).

- Implementing a system of controlling vehicles authorized to park on the premises (e.g., using placards, decals, key cards, cipher locks)

Laboratory safety

- Restricting access to the laboratory.
- Restricting laboratory materials to the laboratory, except as needed for sampling or other appropriate activities.
- Restricting access to sensitive materials.
- Investigating missing reagents or positive controls or other irregularities outside a pre-determined normal range of variability immediately, and alerting local law enforcement about unresolved problems, when appropriate.

Storage and use of hazardous chemicals (e.g., cleaning and sanitizing agents, pesticides, processing aids)

- Securing storage areas for hazardous chemicals (e.g., using locks, seals, alarms etc.)
- Limiting access to storage areas for hazardous chemicals.
- Keeping track of hazardous chemicals
- Investigating missing stock or other irregularities outside a pre-determined normal range of variation.

Employees

Pre-hiring screening

- Screening employees (e.g., obtaining and verifying work references, addresses)
- Performing criminal background checks
- Knowing who is and who should be on premises, and where they should be located
- Being specific to shift
- Keeping information updated
- Establishing a system of positive identification and recognition (e.g., issuing photo identification badges with individual control numbers, color coded by area of authorized access).
- Collecting the retired identification badge when an employee is terminated, either voluntarily or involuntarily.
- Limiting access so employees enter only those areas necessary for their job functions.
- Reassessing levels of access for all employees periodically.

Personal items

- Restricting personal items allowed in establishment.
- Preventing workers from bringing personal items (e.g., lunch containers, purses) into food handling areas
- Establishing policy and providing for regular inspection of contents of employee lockers, bags, and vehicles when on company property.

Training in food security procedures

- Providing food security training to all new employees, including information on how to prevent, detect, and respond to tampering or criminal or terrorist activity.
- Providing periodic reminders of the importance of security procures.
- Ensuring employee buy-in (e.g., involving employees in food security planning, demonstrating the importance of security procedures to the employees themselves).
- Watching for unusual behavior by new employees of workers.(e.g., workers who stay unusually late after the end of their shift, arrive unusually early, access files/information/areas of the facility outside of the areas of their responsibility; remove documents fro the facility; ask questions on sensitive subjects; bring cameras to work)

Appendix II summarized scientific studies

The following section presents the detailed explanation of the scientific researches summarized in Table 3. As it was mentioned in section 3.4, these summarized scientific studies are conducted by different authors in addressing security issues regarding the food supply chain.

Communicating food terrorism[26]

A case report by Van Geest (2002), addressed how to prevent food terrorism. The case was based on a News flash such as "Rat poison found in beer bottles'', "Number of patients rapidly growing: Malice suspected". The author examined the threat whether it is real, deliberate and if so what to be done.

Findings illustrate that policymakers have developed scenarios that identify possible countermeasures and public information aspects of these measures; however, he pointed out that there is lack of co-ordination. He stated as follows: "The Netherlands is a very small country so it is easy for us to co-ordinate action. So far, however, there is hardly any international co-ordination, even though we all know that foods are produced and sold worldwide and, in Europe at least, food problems are often cross-border problems. The European Food Safety Agency is in the process of being set up and one of its primary areas of attention will be communication. Perhaps we should not wait that long and should start exchanging knowledge earlier".

Security assessment and benchmarking too1[27]

One of the NCFPD- funded projects is a research on "Security assessment and benchmarking tool". The goal of this project among others, according to the supply chain best practices team's discussions with food industry firms, is to help companies to understand and organize their supply chain security practices, particularly the often overlooked areas of communication, management support, interaction with suppliers, customers, and carriers. A survey was sent to top 400, food retailers, 400 food service companies, 100 wholesalers for food retailers and for food service companies, 500 top manufacturers, and top trucking firms via internet and mail.

Findings: defense practices at retail food, food service, their wholesale suppliers, manufacturers, and truckers.

- Based on the overall score, foodservice retail ranks number one followed by food service wholesale, grocery wholesale and grocery retail as the most ready sector to defend against intentional risks. The main strength of the food service retail sector is its ability to ensure that their supply chain partners follow jointly established security and food defense protocols. The foodservice wholesale sector outperforms its retail partners by establishing stronger collaboration ties with its supply chain partners and devoting more effort to track and monitor their food products. The only practice where the grocery wholesale sector outperforms the foodservice sector is physical security.
- With regard to firm and supply chain readiness for defending the overall food system, retailers score lower, than manufactures. Manufacturers score lower than foodservice

[26] http://www.fsis.usda.gov/Orlando2002/presentations/ivangeest/ivangeest_text.htm
[27] http://fdrs.ag.utk.edu/07conf/BestPractices.pdf
http://foodindustrycenter.umn.edu/vd/Events/disasterresponsesummary.pdf

- Benchmarking survey of retailers shows intra-company communication and plans are well underway, but communication with suppliers or customers is lacking.

The following examples of best practices were found from the benchmarking survey of retailers:

- All company employees including store, headquarters, warehouse and manufacturing plants go through an FBI background check and drug test.
- Delivery trucks have a number coded plastic seal that breaks every time the door is opened. Each delivery is cross-checked with the corresponding seal.
- Securing the back entrance/exits- locking doors and sealed exit doors with plastic number locks that break when doors are opened.
- Store employees have ongoing training to develop skills to recognize and deal with potential threats.
- Up-to-date list of local first responders posted where any employee can find it in case of an attack.
- Contacts with local, state and federal agencies established in advance.
- Contact with other parts of the company and the supply chain partners established in advance.

Supply chain response to global terrorism: a situation scan[28]

The research was conducted with the objective of investigating how companies perceive the threat of terrorism, how are they assessing and evaluating the related risk for their supply chain, how are companies protecting their supply chain in order to prevent security breaches and how are companies strengthening their supply chain in order to make it more resilient, i.e. more capable of reacting to unexpected disruption? The methodology used to investigate the questions was a semi-structured questionnaire and case studies. 20 companies (medium to large) selected from different industries, operating at different stages of the supply chain for interview. food and beverage industry was one of them.

Findings:

All the interviewed companies are somehow concerned with the potential risk related to the consequences of a terrorist attack on their supply chain, but there is a general sense of disorientation on how to deal with the problem. Managers with responsibilities for both supply chain and security/business continuity are well aware of the many interconnections that link their companies to many others and, consequently, expose them to the risk of suffering from disruptions happening far away. The report shows companies are looking for a way to deal with all these issues. In order to protect the supply chain from disruption, the result shows companies are undertaking a series of initiatives (basic and advanced), such as physical security, information security and freight security. With regard to the issue of supply chain resilience, the report highlighted two main areas of intervention to create a resilient supply chain: company organization and supply network design. Companies pointed out that developing contingency plans and performing specific training and education are the two actions required to achieve resilience within their organizations. As per the report, some of the interviewed companies have some degree of redundancy (duplicating resources to ensure the availability of a backup solution in case of disruption) and have flexibility (the ability to accommodate sudden fluctuations in the availability of resources) in their supply chains as a principles of supply net work design.

[28] http://web.mit.edu/scresponse/repository/euroma_paper_041603.doc.

Defending America's food supply against terrorism: Who is responsible? Who should pay[29]?

A large internet survey of U.S. residents was conducted in August 2005 to provide information about public attitudes and concerns about terrorism and consumers perceptions of food safety and food defense. About 4260 U.S. residents over the age of 16 were completed the interview. Citizens were asked different questions such as how concerned are Americans about food terrorism, who is responsible for food safety and defense, who should pay for food safety and food defense, and how America's anti terrorism budget be allocated.

Findings:

Respondents were given a list of different types of terrorist attacks such as airlines, other public transportation, food, etc. Even though they believe a terrorist attack on the food supply chain to be slightly less likely than other types of terrorism, they devote a greater proportion of the nation's anti-terrorism budget to protect against an attack using the food supply chain than any other types of terrorist attacks. More than 62% of the respondents said, they were not very confident about the security of the U.S food supply against terrorism.

The public also asked to assign responsibility of food safety and food defense to different members of the food supply chain, from farmers to retailers, as well as consumers and the government. The greatest responsibility of *food safety* is assigned to government, food processors and manufacturers where as the greatest responsibility of *food defense* is assigned to government. Respondents also believed that government should bear the cost of food defense and safety. Manufactures and processors were assigned the second highest percentage.

[29] http://www.choicesmagazine.org/2007-1/grabbag/2007-1-12.htm
http://agecon.lib.umn.edu/cgi-bin/pdf_view.pl?paperid=20453&ftype=.pdf

Appendix III Cover letter and questionnaire

Date _____

Geachte Kwaliteitsmanager van _____

Het borgen van kwaliteit en voedselveiligheid wordt steeds belangrijker voor het lange termijn perspectief van agribusiness bedrijven. Besmettingen kunnen leiden tot verstoringen in de voedselketen. Hoe kijken bedrijven in Nederland aan tegen al dan niet bewust veroorzaakte besmettingen? En hoe robuust is de keten om na een grote verstoring weer door te starten? Hoe beter bedrijven dit hebben geregeld, hoe beter hun positie op internationale afzetmarkten. Dergelijke zaken staan centraal in het recent opgestarte onderzoek "**Security and Robustness in Food Supply Chains**". Daarbij richten wij ons op opzettelijk veroorzaakte besmettingen.

Opzettelijk veroorzaakte besmettingen kunnen verschillende oorzaken hebben. Zo kan het gaan om het op dit moment sterk in de belangstelling staande **bioterrorisme**. Maar de opzettelijke aard van een besmetting kan ook voortvloeien uit **tegenstrijdige belangen** tussen bedrijven in de keten, of bijvoorbeeld met werknemers. "Security and robustness" hebben dus zeker met terroristische dreiging te maken, maar het is ons inziens veel breder dan dat.

Om de "Security and robustness" voor een aantal Nederlandse ketens, **van grondstof tot eindproduct**, in kaart te brengen, zouden we u graag willen vragen om bijgevoegde vragenlijst in te vullen (electronisch of op papier). We zouden het bijzonder waarderen als dit lukt **voor 16 november** aanstaande. (De vragenlijst is in het Engels vanwege het internationale karakter van dit onderzoek).

Na afloop van het onderzoek ontvangen alle deelnemers een vertrouwelijke rapportage met daarin opgenomen hun eigen respons afgezet tegen het gemiddelde van de vergelijkbare groep bedrijven. Uiteraard wordt over het onderzoek alleen op geaggregeerd niveau gepubliceerd.

Vertrouwend op uw medewerking,

Gé Backus, LEI
Nico de Groot, LEI
Miranda Meuwissen, Wageningen Universiteit

Retouradres:
Solyana.subuh@wur.nl
Of:
Miranda Meuwissen
Business Economics
Wageningen UR
Hollandseweg 1
6706 KN Wageningen

Security and robustness in food supply chains

I would like first to give a definition of food security.

"*Food security is the process of safeguarding the food system against intentional contamination*". It involves prevention, minimizing, or responding to the deliberate contamination of food products by a variety of potential threats.
In this questionnaire *security* refers to safeguarding the *overall company operation* (e.g. product, premises, workers, process, storage etc.) from intentional contamination.

Intentional contaminations could result from actions of other companies as a result of conflicting interests, employee actions for some personal reasons, or terrorist actions that could lead to unsafe products. It refers to all *purposeful* activities aimed at contaminating products of your company.

INSTRUCTIONS: Please read each statement carefully and circle the number that most describes your company's activity. You can send your responses electronically (e-mail address: solyana.subuh@wur.nl) **or by our postal address which is written at the last page of this questionnaire.**

Part I Company actions

What type of business are you engaged in? Please specify, _____

If you have multiple business units, please specify to which business unit you are referring in completing this questionnaire.

_____

Please take the business unit that you mentioned above to answer the following questions.

- Does your company conduct *security evaluations* to determine weaknesses in production *processes*?

[1] Almost never [2] Rarely [3] Sometimes [4] Usually [5] Almost always

- Does your company conduct *security assessments* for signs of tamper with products?

[1] Almost never [2] Rarely [3] Sometimes [4] Usually [5] Almost always

- How often does your company make *security assessments* to the *overall operation*?

[1] Almost never [2] Rarely [3] Sometimes [4] Usually [5] Almost always

- How often does your company evaluate *suppliers' activities* with regard to securing their overall operation?

[1] Almost never [2] Rarely [3] Sometimes [4] Usually [5] Almost always

Please circle the number that describes your level of agreement with the following statements:

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Not applicable
Our company has implemented security control mechanisms for *its employees* (e.g., background checks, working history, storage of personal items, etc.).	1	2	3	4	5	6
Our company has implemented security control mechanisms (e.g., badges, permits, uniforms identification cards, etc.) for *external parties* (e.g., visitors, external technicians, etc.).	1	2	3	4	5	6
Our company has restricted access to key *facilities* (e.g. water, computer software, etc).	1	2	3	4	5	6
Our company restricts access to sensitive areas (e.g., laboratory, open product areas, etc).	1	2	3	4	5	6
Our company has assigned a *responsibility* to qualified individuals to handle security related issues.	1	2	3	4	5	6
Our company has implemented procedures to ensure the security of incoming packages and materials.	1	2	3	4	5	6

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Not applicable
Our company continuously evaluates the vulnerability of its logistics system for security related risks.	1	2	3	4	5	6
Our company requests locked and/or sealed containers/vehicles from its suppliers and transporters.	1	2	3	4	5	6
Our company issues identity cards, company clothes and badges for its employees for security purpose.	1	2	3	4	5	6
Our company provides an appropriate level of *supervision t*o all its employees including contract workers, data entry, cleaning and maintenance staff.	1	2	3	4	5	6
Our company requests *ISO 22000:2005,* (International standardization organization) *certification* and registration of companies to ensure the safety of products.	1	2	3	4	5	6
Our company implemented *ISO 28000:2005* which specifically deals with *security* of supply chains.	1	2	3	4	5	6

- What *other certifications* does your company require from its suppliers?

[1] GMP+ (Good Manufacturing Feed Practice) [2] SQF (Safe Quality Food) [3] BRC (British Retail Consortium)

[4] IFS (International Food Standards) [5] others, please specify _____

- Does your company operate with a *Hazard Analysis and Critical Control Point* (HACCP) System?

[1] Yes [2] No [3] Do not know

- What *guidelines* does your company adopt to control security of products?

[1] HACCP [2] FSIS (Food Safety and Inspection Service) [3] IFDA (International Food Distribution Association) [4] Others, please specify_____

- Are there any *other requirements* or procedures that must be followed in your company in order to protect the company from intentional risks?

[1] Yes [2] No [3] Do not know

- If your answer to the above question is "Yes", what *kind of requirements*?

[1] Government requirements [2] Industry requirements [3] Company specific requirements [4] All

[5] Other, please specify_____

- If your answer to the above question is "3", "company specific", please mention them.

_____

_____

- Does your company implement procedures to investigate information regarding suspicious activities (e.g., unscheduled deliveries, unusual packages, mails, etc.) related to security risks?

[1] Yes [2] No [3] Do not know

	Almost never	Rarely	Some times	Usually	Almost always
Does your company inspect suppliers' *plants* regarding security related risks?	1	2	3	4	5
Does your company conduct *security tests* on *suppliers' operations* (e.g., manufacturing, storage, movement of products etc.)?	1	2	3	4	5
Do you think that the rules of *hygiene and food safety* are respected by your suppliers?	1	2	3	4	5

Please circle the number that describes your level of agreement with the following statements:

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Not applicable
Our company has implemented *standards* to asses suppliers' performance with regard to protecting the supply chain from security related risks.	1	2	3	4	5	6
Our company *verifies* that suppliers and transporters perform *background* checks on their employees.	1	2	3	4	5	6
Our company *verifies* that suppliers and transporters use *government and industry security guidelines.*	1	2	3	4	5	6
Our company uses *its own audit team* to verify the security procedures of supply chain partners.	1	2	3	4	5	6
Our company uses *third party audit team* (as opposed to self-audits) to verify the security procedures of supply chain partners.	1	2	3	4	5	6
Our company has implemented plans on how to *continue its operation* in case of lack of availability of facilities (e.g. electricity, water, transportation communication and internet) due to security related incidents occurring along the supply chain.	1	2	3	4	5	6
Our company has designed plans on how to *continue its operation* in case of lack of availability of raw materials.	1	2	3	4	5	6
Our company has *emergency budgets* to carry on its operations in case any security related incidents occur along the supply chain.	1	2	3	4	5	6
Our company maintains *records* that demonstrate who is manufacturing, processing, packing, and transporting, distributing, receiving and holding products.	1	2	3	4	5	6
Our company maintains a *list of local and national emergency contacts* to notify any intentional acts including suspicions.	1	2	3	4	5	6
Our company is working with *nationwide organizations* to counteract any intentional risks.	1	2	3	4	5	6
Our company is working with *international organizations* to counteract any intentional risks.	1	2	3	4	5	6
Our company is working with government agencies (e.g., Ministry of Health, Ministry of Agriculture, etc.) to prevent and respond to any security related risks.	1	2	3	4	5	6

Part II Performance

Please circle the number which could evaluate the performance of your company and the supply chain as a whole.

	Very good	Good	Neutral	Poor	Very Poor
How would you rate your company's performance in *securing premises* from security related risks/incidents?	1	2	3	4	5
How would you rate your company's *responsiveness* to any intentional risks/incidents?	1	2	3	4	5
How would you rate the activities done by your company so far to *prevent* and *protect* the company *processes* from intentional risks?	1	2	3	4	5
How would you rate the overall supply chain *readiness* to respond to any intentional risks?	1	2	3	4	5
How would you rate the overall performance of your company with regard to *actions* undertaken so far to secure the company from security risks?	1	2	3	4	5
How would you rate the *relationship* you have with your *suppliers* with regard to *sharing information* regarding security risks*?*	1	2	3	4	5
How would you rate the *relationship you have* with *customers* with regard to *sharing information* related to security risks*?*	1	2	3	4	5
How would you rate your *relationship* with *government agencies* with regard to *sharing information* related to security risks*?*	1	2	3	4	5

- How would you rate the overall satisfaction with your suppliers' *responsiveness* to security related risks occurred along the supply chain?

[1] Very unsatisfied [2] Unsatisfied [3] Undecided [4] Satisfied [5] Very satisfied

Part III Information sharing

- What kind of information does your company share with *suppliers* with regard *to intentional risks*

Before accident occurs _____

_____

After accident occurs_____

- What kind of information does your company share with *customers* with regard *to intentional risks*?

Before accident occurs _____

_____

After accident occurs_____

- What *motives/incentives* do you have to share *security related information* with *suppliers*?

[1] Protect brand image [2] Limit liability exposure [3] Avoid penalties [4] All

[5] Others, please specify_____

_____

- With whom does your company mainly share security related information?

[1] Suppliers [2] Government [3] Customers [4] All [5] Others, please specify_____

Please circle the number that describes your level of agreement with the following statements:

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Not applicable
Our company's information systems provide managers the *timely* information they need to respond to intentional incidents**.**	1	2	3	4	5	6
Our company shares information regarding *sources of products* with its customers.	1	2	3	4	5	6
Our company shares information about the *security of products* with its customers.	1	2	3	4	5	6
Our company's *information systems* allow us to quickly share appropriate information to all company employees in case of security incidents.	1	2	3	4	5	6
Our company has established a *communication strategy* for providing information about intentional risks/incidents to supply chain partners.	1	2	3	4	5	6
Our company's information systems provide managers *consistent* information to respond to intentional risks/ incidents.	1	2	3	4	5	6
Our company has complete *information* about *its suppliers* operation. (e.g., how they are working, sources of raw materials, with whom they are working).	1	2	3	4	5	6
Our company has designed *awareness* programs for *supply chain members* regarding security issues.	1	2	3	4	5	6
Our company has established a clear *communication procedure* to be used by its suppliers in case of security related incidents.	1	2	3	4	5	6
Our company has designed *training programs* for its *employees* on how to *protect from* and *respond to* security risks/ incidents.	1	2	3	4	5	6

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Not applicable
Our company has a *senior management* position focusing on security (e.g., Director of Security, Chief Security Officer).	1	2	3	4	5	6
Our company has adopted an *incentive system* (e.g. financial rewards, recognition etc.) for its employees and supply chain members for *compliance with* supply chain security procedures.	1	2	3	4	5	6
Our company has established *consequences* for *employees* who fail to comply with internal security procedures**.**	1	2	3	4	5	6
Our company has adopted a *penalty system* (e.g. fines, product recall and public announcement, temporary/permanent restrictions etc) for its suppliers for non-compliance to supply chain security procedures.	1	2	3	4	5	6

- Did your company ever face any product recalls with regard to ***un****intentional contaminations*?

  [1] Yes [2] No [3] Do not know

- Did your company ever face any product recalls with regard to *intentional contaminations*?

  [1] Yes [2] No [3] Do not know

- If your answer is "Yes", how many times did your company face a recall in the past five years with regard to *intentional risks*? (In numbers)

  [1] 1 [2] 2-5 [3] 6-10 [4] 11-15 [5] >15 [6] Do not know

- What kind of supplier selection criteria does your company use?

  [1] Low- cost [2] Quality [3] Both [4] Other, please specify_____

- How many suppliers do you have?

  [1] 1-5 [2] 5-10 [3] 11-20 [4] 20-30 [5] 30-50 [6] >50

- Does your company conduct security issue meetings with suppliers?

  [1] Never [2] Rarely [3] Sometimes [4] Usually [5] Always

- For how long did your company work with your main suppliers? (In years)

  [1] 0-1 [2] 2-5 [3] 6-10 [4] 11-15 [5] >15 [6] Do not know

- How do you rate the general *awareness level of your suppliers* on *how to communicate* in case of security related incidents along the supply chain?

  [1] Very good [2] Good [3] Neutral [4] Poor [5] Very poor

- How would you rate the *trust level* you have with your *suppliers*?

  [1]Very good [2] Good [3] Neutral [4] Poor [5] Very poor

- Our company is very *committed* to *maintain the relationship* it has with its suppliers.

  [1] Strongly disagree [2] Disagree [3] Neutral [4] Agree [5] Strongly agree

- Renewal of the *delivery contract* with our suppliers is almost *automatic*.

  [1] Strongly disagree [2] Disagree [3] Neutral [4] Agree [5] Strongly agree

- How would you rate the overall work *relationship* you have with your *suppliers*?

  [1]Very good [2] Good [3] Neutral [4] Poor [5] Very poor

- How do you rate the *trust* level you have with your *employees*?

  [1]Very good [2] Good [3] Neutral [4] Poor [5] Very poor

- Our company views supply chain security as an *objective* for securing:

  [1] Brand reputation [2] Competitive advantage [3] Market growth [4] all [5] Other, please specify____

Please circle the number that describes your level of agreement with the following statements:

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Not applicable
Our company uses *Radio Frequency Identification (RFID)* to effectively track the products in our control.	1	2	3	4	5	6
Our supply chain partners *collaborate* in the use of radio frequency identification (RFID) to track products throughout the supply chain.	1	2	3	4	5	6
Our company has the ability to *track and trace* products *one supplier up and one supplier down* the supply chain.	1	2	3	4	5	6
Our firm uses t*echnology* (e.g., X-ray) to verify trailer or container contents.	1	2	3	4	5	6
Our company has the *technology (e.g., bar-coding, RFID etc.) to track* reworked and returned products.	1	2	3	4	5	6

Part IV Background

- Your title? _____

- Your main functional area?

[1] Operations [2] Quality Assurance [3] Security [4] Risk Management [5] Other, please specify _____

- Your work experience in the industry (in years)?

[1] 0-1 [2] 2-5 [3] 6-10 [4] 11-15 [5] 16-20 [6] > 20

- Work experience in your current position (in years)?

[1] 0-1 [2] 2-5 [3] 6-10 [4] 11-15 [5] 16-20 [6] > 20

- Did your company ever face ***un****intentional* contaminations?

[1] Yes [2] No [3] Do not know

- If your answer to the above question is "Yes", how many times did your company face the risk during the past five years?

[1] One [2] Two [3] Three [4] 4 and above [5] Do not know

- Did your company ever face *intentional* contaminations?

[1] Yes [2] No [3] Do not know

- If your answer to the above question is "Yes", how many times did your company face the risk during the past five years?

[1] One [2] Two [3] Three [4] 4 and above [5] Do not know

- How do you perceive the intentional contamination?

[1] Sever [2] Moderate [3] Mild [4] Very mild [5] None [6] Do not know

- Do you think an intentional risk is a threat to your company?

[1] Yes [2] possibly [3] No [4] Do not know

-Considering the issue of intentional attacks, how risky would you say the food supply chain is in the Netherlands?

[1] Not risky at all [2] Not much risk [3] Moderate [4] Risky [5] Very risky [6] Do not know

END

Appendix IV Security performance feedback to respondents

(Shortened version)

Table 1: Number of respondents.

	Number of companies returned the questionnaire
Feed	11
Seed	2
Pork (processing)	3
Vegetable (processing)	4
Wholesale/retail	3
Total	23

Table 2: Company's risk perception on the occurrence of intentional risk (%).

	Very (risky)	Moderately risky	Not risky
Company level	27	55	18
Country level	10	35	45

Table 3: Company's experience with regard to intentional and unintentional contaminations.

Intentional contamination (%)	Recall due to intentional contamination (%)	Unintentional contamination (%)	Recall due to unintentional contamination (%)
24	23	77	62

Table 4: Perceived security performance score and your company's score.

	Overall mean (n=23)	Feed (n=11)	Seed (n=2)	Meat processing (n=3)	Vegetable processing (n=4)	Wholesale/ retail (n=3)	**Your Company (X)**
Information sharing[1]							
Communication management	2.64	2.76	1.83	2.89	1.92	3.44	**x**
Management technology	3.59	3.67	2.88	3.72	3.61	3.61	**x**
Relationship management	2.64	2.76	1.50	3.22	2.42	2.67	**x**
Public interface management	3.26	3.41	1.92	3.19	3.32	3.61	**x**
Control actions[2]							
Process strategy	3.00	3.00	2.00	3.17	3.00	3.50	**x**
Process management	2.77	3.03	1.75	2.25	2.74	3.08	**x**
Process technology	2.86	2.78	2.30	3.02	3.00	3.13	**x**
Metrics	2.70	3.27	1.50	1.33	3.00	3.33	**x**
Infrastructure management	3.16	3.10	2.96	2.84	3.35	3.54	**x**
Robustness[3]							
Continuation plans incase of lack of facilities	3.26	3.00	4.00	3.67	3.00	3.67	**x**
Continuation plans incase of lack of raw materials	3.27	3.20	3.00	3.00	3.50	3.67	**x**
Emergency budgets to continue operations	3.09	2.90	2.50	4.00	3.50	2.67	**x**
Company's own performance evaluation[4]	3.18	3.31	2.67	2.81	3.18	3.48	**x**

[1] For more detailed scores see table 5.
[2] For more detailed scores see table 6.
[3] For more detailed scores see table 7.

[4] For more detailed scores see table 8.

Table 5: Perception about own company's information sharing practice in the field of security (n=23).

Our company …	Strongly disagree (%)	Disagree (%)	Neutral (%)	Agree (%)	Strongly agree (%)
Communication management					
Designed awareness programs for chain members	9	46	36	9	-
Established communication procedures for suppliers	9	18	26	36	9
Designed training programs for employees	5	45	32	18	-
Management technology					
Implemented IS[1] that provide timely information	9	14	14	59	4
Implemented IS[1] that provide consistent information	4	9	32	46	9
Impl. IS[1] that quickly share info with all employees	-	-	18	73	9
Impl. a communication strategy for chain partners	9	14	13	59	5
Shares info on sources of products with customers	5	9	18	46	23
Shares info on security of products with customers	-	5	32	46	18
Relationship management					
Adopted incentive systems[2] for chain members	29	52	14	5	-
Adopted consequences for employees' non-compl.	13	9	27	46	5
Adopted penalty system for suppliers' non-compl.	19	19	10	38	14
Public interface management					
Maintains records on company's processes[3]	4	9	4	57	26
Has complete information on suppliers' operations[4]	9	14	36	36	5
Maintains list of local/national emergency contacts	9	13	13	48	17
Works with nat. org. to counteract intentional risks	8	22	39	22	9
Works with internat. org. to counteract intent. risks	24	19	24	24	9
Works with gov. for risk prevention and response	17	4	35	35	9

[1]IS: Information systems.
[2]Such as financial rewards and recognition.
[3]Such as on who is manufacturing, processing, packing, transporting, distributing, receiving, holding products.
[4]On issues such as how they are working, sources of raw materials, with whom they are working.

Table 6: Perception about own company's control actions in the field of security (n=23).

Our company …	Strongly disagree (%)	Disagree (%)	Neutral (%)	Agree (%)	Strongly agree (%)
Process strategy					
Has a senior management position on security	19	57	5	14	5
Assigned responsibility to qualified individuals	13	9	4	61	13
Process management					
Requests ISO22000:2005 certification from suppliers	26	53	11	5	5
Implemented ISO28000:2005	35	59	6	-	-
Impl. standards to asses suppliers' performance	9	18	23	36	14
Verifies suppliers' background checks on employees	18	50	14	18	-
Uses own audit team to verify procedures in chain	18	23	27	27	5
Use 3rd party audit team to verify procedures in chain	14	27	13	32	14
Inspects suppliers' plants*	39	18	17	26	-
Conducts security tests on suppliers' operations*	35	22	8	35	-
Beliefs suppliers to respect hygiene and safety rules*	5	-	4	68	23
Process technology					
Uses RFID to track products	52	29	14	5	-
Works with suppliers using RFID	50	30	5	10	5
Is able to track and trace products[1]	-	4	4	22	70
Uses technology to verify trailer/container contents	61	28	-	11	-
Has technology to track reworked and returned pr.	17	13	9	48	13
Metrics					
Verifies suppliers' use of security guidelines*	23	23	9	41	5
Infrastructure management					
Conducts security evaluations to determine weaknesses in production processes*	18	9	27	23	23
Conducts security assessments for signs of tamper with products*	30	15	20	10	15
Makes security assessments of the overall operation*	23	9	27	32	9
Evaluates suppliers' overall operation*	26	9	21	22	22
Continuously evaluates logistics system	13	17	39	31	-
Implemented control mechanisms for employees[2]	13	13	30	35	9
Implemented control mech. for external parties[3]	13	13	17	44	13
Restricted access to key facilities (water, control unit)	4	4	9	78	4
Restricted access to sensitive areas (lab, open product)	4	9	18	55	14
Implemented procedures for incoming materials	9	14	23	36	18
Requests locked/sealed containers from suppliers	17	48	13	17	4
Issues identity cards/cloths/badges for employees	9	14	36	32	9
Provides appropriate supervision to all employees[4]	4	13	26	44	13

*Answers were on a liker-scale, i.e. 1 (almost never), 2 (rarely), 3 (sometimes), 4 (usually) and 5 (almost always).
[1]Tracking and tracing of products "one supplier up and one supplier down the supply chain".
[2]Such as background checks, working history and storage of personal items.
[3]Such as badges, permits, uniforms and identification cards.
[4]Including contract workers, data entry, cleaning and maintenance staff.

Table 7: Perception about own company's robustness in the field of security (n=23).

Our company …	Strongly disagree (%)	Disagree (%)	Neutral (%)	Agree (%)	Strongly agree (%)
Implemented plans for business continuation in case of lack of availability of facilities[1]	4	22	22	48	4
Implemented plans for business continuation in case of lack of availability of raw materials	-	27	22	45	4
Has emergency budgets to continue operations	-	27	41	27	5

[1]Such as electricity, water, transportation, communication and internet.

Table 8: Perception about company's own and overall chain performance in the field of security (n=23).

How do you rate your company's …	Very poor (%)	Poor (%)	Neutral (%)	Good (%)	Very Good (%)
Performance in securing premises	4	18	30	39	9
Responsiveness	-	13	32	46	9
Activities to protect processes	4	5	64	18	9
Overall performance	4	17	26	44	9
Relationship with suppliers with regard to sharing information	5	30	26	30	9
Relationship with customers with regard to sharing information	-	35	26	30	9
Relationship with government with regard to sharing information	-	22	30	39	9
Suppliers' awareness level and communication	4	44	30	18	4
Supply chain readiness to respond	-	35	35	26	4