Security and robustness in food supply chains

Solyana A. Subuh[1], Miranda P.M. Meuwissen[1], Paul T.M. Ingenbleek[2], Gert-Jan Hofstede[3], Ge B.C. Backus[2]

[1]Business Economics, Wageningen UR, Hollandseweg 1, 6706 KN Wageningen, The Netherlands, 31 317 483857, solyana.subuh@wur.nl, miranda.meuwissen@wur.nl

[2]Agricultural Economics Research Institute (LEI), Wageningen UR, Hollandseweg 1, 6706 KN Wageningen, The Netherlands, 31 317 484491, paul.ingenbleek@wur.nl, ge.backus@wur.nl

[3]Information Technology Group, Wageningen UR, Hollandseweg 1, 6706 KN Wageningen, The Netherlands, 31 317 484630, gertjan.hofstede@wur.nl

Abstract

Food security issues are generally discussed from a US perspective and mostly focus on terrorism. This paper shows the results of an exploratory study on more broadly defined security risks for meat and vegetable supply chains in the Netherlands. Meat supply chain respondents reflect 58% (feed), 38% (processing) and 17% (wholesale/retail) of sector capital. Findings show that only about one-third of the companies regards security risks as a real threat. Also, food safety assurance programs are mistakenly interpreted as tools for food security prevention and there is little cooperation at national and international level. In terms of robustness, about 50% states to have emergency plans. From a supply chain management point of view, results indicate the explicit need for security awareness and preparedness programs, both at company level as well as for food supply chains as a whole.

Keywords: Intentional risks; Control actions; Information sharing, Security performance

1. Introduction

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, which includes a 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 the existence of these new certification schemes, a recent US security assessment study recognized that areas of communication, management support and interaction with suppliers, customers and carriers are often overlooked (Kinsey et al., 2007). Also, in a case study on communication practices in case of food terrorism (Van Geest, 2002), it was concluded that there is a lack of international coordination. Furthermore, Sheffi et al. (2003) and Closs et al. (2006) illustrate that companies and institutions generally focus on terrorists' actions. FSIS (2007), however, points out that intentional threats can be from a much wider range of sources such as dissatisfied employees and suspected suppliers.

In this framework, our paper aims at exploring security performance of food supply chains in a wider context, i.e. food security risks are defined as intentional risks caused by various parties such as terrorists, supply chain partners with conflicting interests and dissatisfied employees. Companies are from the meat and vegetable supply chain and have (part of) their business in the Netherlands. Their 2002-2004 average total capital was at least Euro 4 million.

To illustrate the case of the paper, section 2 presents a number of intentional threats to food supply chains from recent history. This section also highlights some of the key differences between the concepts of food safety versus food security. Section 3 discusses the conceptual framework on security performance. In section 4, questionnaire design and sample are presented. Section 5 and 6 include detailed and more aggregated results respectively. Conclusions and discussion are in section 7.

2. Food security risks

2.1 Some examples of security risks in food supply chains

Purposeful contamination of food can occur at anytime 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 (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 was stated 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 competitor's breakfast foods with rat poison resulting in 40 deaths and 200 hospitalizations in Nanjing, 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, owners of a noodle factory contaminated their food with rat poison, sickening 120. In Canada in 1970, a postgraduate student contaminated his roommates' food with *Ascaris suum* (a parasite). Four of the victims became seriously ill.

More generally, Coleman (2004) describes three types of intentional threats to food supply chains, i.e. (1) 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; (2) the introduction of anti-crop or anti-livestock agents into agricultural systems; and (3) the physical disruption of the flow of food or water as a result of the destruction of transportation or other vital infrastructure. Deliberate biological or chemical contamination of food or water, i.e. "threat (1)", is generally regarded as the easiest method for widespread terrorism. Chemicals, heavy metals, such as lead and mercury, and living organisms, such as bacteria and viruses, can all be threats to a safe water supply (Bryson, 2005). With regard to "threat (2)", the WHO (2002) states that, despite the importance of agriculture to economy and well-being of citizens, limited attention has been given so far to the agricultural vulnerability to individual or terrorist attacks. WHO (2002) furthermore states that, with respect to "threat (3)", i.e. the physical disruption of the flow of food and water, this is a critical area and possibly the area that has the least amount of protection currently.

2.2 Food security versus food safety

Food safety and food security both deal with the safety of food. Their main difference lies in the nature of the risk, i.e. food safety deals with unintentional risks, while food security deals with intentional risks. Similarly, authors regard food safety threats as threats that can be reasonably anticipated, while food security threats are often seen as very difficult to anticipate. There is however a long list of food safety assurance systems, such as HACCP, BRC, EUREP-GAP and ISO22000:2005, while the number of food security systems is very limited. We identified two schemes, i.e. AEO and ISO28000:2005. In addition, there is a "farm-to-table security assessment tool" entitled CARVER+shock. This tool was developed (and applied) in the US and adapted from a military version. CARVER is an acronym for six attributes used to evaluate the attractiveness of a target for attack: (1) criticality, as a measure of public health and economic impact of an attack; (2) accessibility, as a measure for the ability to physically access and egress from target; (3) recuperability, referring to the ability of a system to recover from an attack; (4) vulnerability, which refers to the ease of accomplishing an attack; (5) effect, measuring the amount of direct loss from an attack as measured by loss in production; and (6) recognizability, referring to ease of identifying the target. A seventh attribute, "Shock", was added to assess the combined health, economic and psychological impacts of an attack within the food industry (FDA, 2007).

3. Conceptual framework on measuring security performance

The conceptual framework has been developed along the central lines of risk management: risk prevention, i.e. preventing a risk from occurring, and risk mitigation, i.e. minimizing the (economic) consequences once a risk has occurred. Combining these concepts with the security framework of Closs (2005), we identified three major categories of competencies that contribute to a food company and food chain security performance. These are the categories of control actions, information sharing and robustness. With regard to *control actions*, relevant competencies are (following Closs, 2005):

- *Process strategy*, which refers to a company's philosophy regarding the importance of food supply chain security. This includes different characteristics such as a company's senior management commitment to security and assigning a senior management position and commitment to security. Other items are to encourage security culture as a necessary condition for implementing an effective security management and considering security as a means to provide competitive advantage, i.e. necessary to protect brand and cost of doing business.
- *Process management*, referring to how people do things, including for instance procedures for dealing with internal operations, employing security guidelines from FSIS, testing supply chain protection capabilities and employing HACCP throughout the supply chain.
- *Process technology*, referring to diagnostics and tracking systems to monitor processes. This includes the use of RFID technology to track products including salvaged, reworked and returned products.
- *Infrastructure management*, which refers to the manner in which a company secures its premises and products. This includes among others the presence of gates, guards, fences, seals on containers and trailers and security checks on and access control of employees. Also, this includes maintaining empty trailers in a secure environment and access control to critical company infrastructure.
- *Security measurement*, including guidelines on how security is measured. This includes implementing industry, company and government guidelines regarding supply chain security.

With regard to the category of *information sharing*, critical competencies included in our framework are (adapted from Closs, 2005):

- *Communication management*, referring to training, education and internal communication on food security awareness and response.
- *Management technology*, which includes information technology with regard to security at the company and supply chain level. Technology should be able to provide valid and timely information to supply chain partners in case of security incidents.
- *Relationship management*, referring to relationships with suppliers and customers. This includes the use of supply chain security audits for frequently used suppliers, the use of historical information from security audits to determine if relationships should be maintained and application of specific educational programs regarding security procedures.
- *Public interface management*, pointing at the relationships with government and the public. This includes participation in emergency preparedness planning with appropriate government agencies, collaboration with public health groups, and establishing a risk communication strategy for the media.

In our conceptual framework, *robustness* is captured by the competencies of whether or not a company has emergency plans and whether there is some emergency budget. Figure 1 graphically presents the framework.

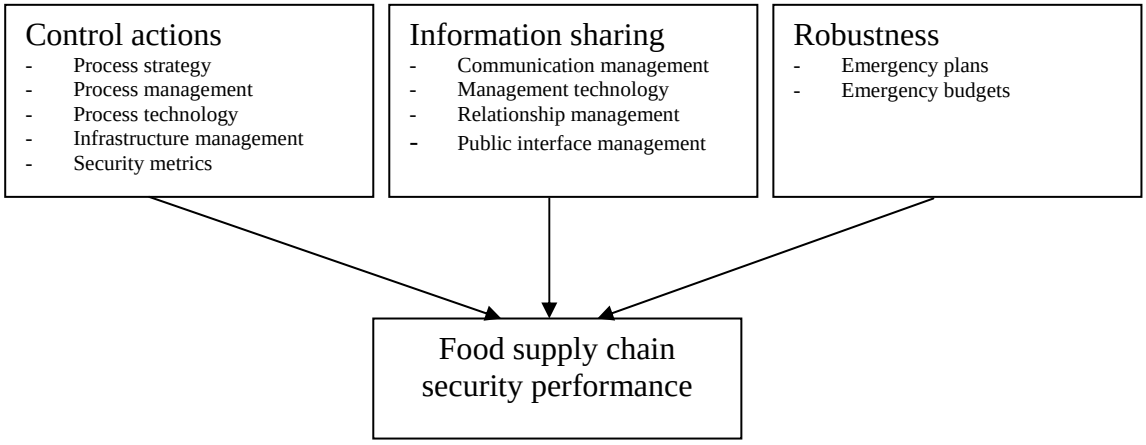

Figure 1: Conceptual framework for measuring perceived security performance of food supply chains.

4. Materials and methods

4.1 Questionnaire design

In order to elicit companies' perceptions about their security performance, a semi-structured questionnaire was designed. There were about 100 questions, subdivided into four parts in the following order: (1) *control actions*, including questions about activities such as security control of the company's overall operation, inspection of suppliers' plants, and risk awareness programs for employees and supply chain members; (2) *company, supplier and supply chain security performance* in which companies were asked to evaluate their own performance in preventing and mitigating intentional risk, as well as the perceived performance for suppliers and the supply chain as a whole; (3) *information sharing*, including questions such as the kind of information (pre and post risk) that companies share with their chain members, the motives they have to share such kind of information and the kind of information sharing technology used; and (4) *background information* in which we asked questions about the company's own

risk experience during the past five years and companies' perceptions about intentional contaminations. In the last section also title, functional area and work experience of respondents were enquired. The questions for robustness were incorporated in the part on control actions. In each question we stressed to focus on *security* risks, which were clearly defined at the beginning of the questionnaire as *intentional* risks caused by *various* parties such as terrorists, supply chain partners with conflicting interests and dissatisfied employees.

Throughout the questionnaire, a combination of closed and open-ended questions was used. Closed questions were in the form of statements for which answers could be indicated on 5-points likert scales. Open-ended questions were used to get insight into such issues as the parties with whom information about intentional risks is shared, the exact kind of information shared with suppliers and customers pre and post intentional risks, and the reason for sharing this information. The questionnaire was pre-tested with three experts from different food companies in order to test the questionnaire for clarity of the statements and need for additional ideas. Comments and suggestions given 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. In the cover letter it was stressed that intentional risks in the survey do not only refer to threats of terrorists but also to threats potentially caused by dissatisfied employees or other supply chain partners with conflicting interests. Telephone was used for follow up of non-response. The complete questionnaire and cover letter are available with the authors.

4.2 Sample

In November 2007, the questionnaire was sent to 130 companies from two sectors, i.e. meat and vegetables. Companies in the meat sector included feed companies and meat processors. For the vegetable sector these were seed companies and vegetable processing companies. Also, we incorporated wholesale/retail. Companies selected have greater than 4 million average total capital for the period of 2002-2004. To select these companies and their respective financial status, a database from Agricultural Economics Research Institute (LEI) was used. The response rate is 18%, i.e. 23 companies returned the questionnaire, including 14 companies from the meat sector, 6 companies from the vegetable sector and 3 from the wholesale/retail part. These response numbers are relatively low. However, considering the average sector capital represented, i.e. 58% (feed), 38% (meat processing), 23% (seed), 9% (vegetable processing) and 17% (wholesale/retail), response data is regarded as fairly representative for meat and vegetable supply chains in the Netherlands.

4.3 Method of analysis

Because of the exploratory nature of this study, descriptive statistics such as frequency tables and compare means such as t-test analyses were used. Frequency tables were used to describe issues such as how many of the respondents conduct security practices and share information related to security risks with their employees, suppliers and customers. Independent sample t-tests were used to test whether there is a difference in security practice between the two sectors (meat versus vegetable), the supply (seed and feed) versus process/retail stages of the food supply chain and the companies with past experience regarding intentional contaminations versus those who had not.

5. Results per security measuring variable

5.1 Risk experience and perception

At *country* level, intentional risks are perceived as (very) risky by 10% of the respondents. 35% regards intentional risks as moderately threatening and 45% perceives these risks 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% had related recalls. With respect to *un*intentional risks, these numbers are 77% and 62% respectively.

5.2 Control actions

Results in the category of control actions show that companies generally 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 operates with HACCP based systems. Also, 60% of the respondents indicates that there are other industry, government or company specific guidelines and requirements to achieve supply chain security. However, 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 1 shows companies' perceptions about their own 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 does not have a senior management position focusing on security. With regard to *process management* none of the respondents implemented ISO28000:2005. In addition, 57% of the respondents does not conduct inspection on suppliers' operations and plants with regard to intentional risks. Companies (91%) believe that their suppliers respect hygiene and safety rules. In relation to *process technology* 81% of the respondents does 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 restricts access to key facilities. Companies seem to be more confident in controlling external parties than internal staff. However, above 50% of the respondents indicates that they provide appropriate supervision to all employees, including contract workers, cleaners and data entry staff. Moreover, 68% (not in Table 1) of the respondents evaluates their trust level with employees as good.

Table 1: 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 different likert-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.

5.3 Information sharing

Companies seem not to extensively share information with suppliers and customers. In answering 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" 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 is shared with suppliers and customers regarding intentional contaminations. In responding to our question "with whom do you mainly share", 31% of the respondents mainly share with their suppliers, 16% with government, 15% with customers and 38% with all, i.e., suppliers, government and customers. These figures however seem to contrast with our finding that about 80% of the respondents never conducts security meetings with chain partners.

Table 2 shows companies' perceptions about their information sharing practices. 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 enables them to quickly and consistently share information with their employees and chain partners. Also, more than 60% of the respondents indicates 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'. 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 2: 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.

5.4 Robustness

With regard to companies' ability to recover from and continue their operation whenever security related risks occur, Table 3 shows that companies generally seem to be somewhat 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 agrees to have emergency budgets to continue operations in case an incident occurs.

Table 3: 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 Companies 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 minimizing losses of such risks after occurrence. With respect to the relationship with suppliers, companies (91%) evaluate their overall work relationship with suppliers' as good and 69% (strongly) agrees to be committed to maintain the relationship. Also, 64% of the respondents qualifies their trust level with suppliers as good. However, only 39% of the respondents agrees to have automatic renewals of delivery contracts with suppliers. Regarding companies overall satisfaction, only 38% of the respondents is satisfied with suppliers' responsiveness to security and 35% (Table 4) qualifies supply chain readiness to respond to intentional risks as poor. Also, companies (44%) regard the suppliers' awareness level and communication in the field of security related risk as poor. With respect to the own company's security performance, unlike suppliers' responsiveness, Table 4 indicates that 46% of the respondents rates their responsiveness to security risks as good.

Table 4: 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 wrt sharing information	5	30	26	30	9
Relationship with customers wrt sharing information	-	35	26	30	9
Relationship with government wrt 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

6. Aggregated results per competency

6.1 Performance scores per competency

Before grouping the individual measuring variables per competency (see Tables 1 to 4), first a reliability analysis for testing internal consistency was performed. Identified Cronbach's alpha values were: communication management (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) and company's own performance (0.878). Because of the low value for robustness, it was decided to consider the three variables classified under robustness separately.

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. Results are shown in Table 5. In the category of control actions, infrastructure management (e.g. restricting access to key facilities and sensitive areas) outperforms all the other competencies while metrics get the lowest score. Pairs that significantly differ 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). In

the category of information sharing, management technology significantly ($P \leq 0.1$) outperforms all the other competencies while communication management gets the lowest score. In the category of robustness, no significant differences are identified.

Table 5: Cross-comparison of the overall mean scores of the competencies by category.

	Overall mean (n=23)[1]
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]
Information sharing	
Communication management	2.64 [a]
Relationship management	2.64 [a]
Public interface management	3.26
Management technology	3.59
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.

6.2 Relationship between the categories of competencies

To test the relationship between the categories (control actions, information sharing, plans in case of lack of facility, plans in case of lack of raw materials and emergency budgets) a correlation test has been performed. Results reveal that all the categories are positively correlated ($P \leq 0.10$). This indicates that 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 (control actions, information sharing and robustness) of the conceptual framework. The hypothesis was that results of these categories should be comparable to the companies' own performance evaluation. Correlation results revealed 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. This indicates that our evaluation of companies' performance regarding security is highly comparable with their own security performance evaluation, which strengthens our analyses.

6.3 Differences across chains and chain stages

Results of the sample t-tests for *meat versus vegetable* chains show that (Table 6) with public interface management the meat sector outperforms the vegetable sector in activities such as maintaining records on company's processes, maintaining information about suppliers operations and working with national and international organizations. All the other competencies do not show a significant difference between the two sectors. Also, when comparing *supply versus wholesale/retail* partners of the chain, we identify only one variable that significantly differs between the two, i.e. the variable with respect to emergency budgets to continue operations after a crisis.

In Table 6 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

security 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.* By considering companies past risk experience with regard to intentional risks, the hypothesis was that those companies who faced the risk in the past would perform better in securing their company and food supply chain. We now see a significant difference in performance scores between those companies who faced intentional contaminations during the past five years and those who did not. Five of the competencies, i.e. *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' operations and requests for certification; *process technology*, which includes implementation of technologies such as RFID; *metrics*, which refers to verifying 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 for employees and external parties show significant differences ($P \leq 0.10$). Company's own performance evaluation also shows a 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, emergency budgets to continue operations show a lower score for companies who have past risk experience. This might indicate that those who faced the risk might actually better know how to handle the risk and how much is needed to maintain for emergency.

Table 6: Mean scores of the two sectors (meat and vegetable), stages (supply and process/retail) and "degree of experience with intentional contaminations". Bold figures represent statistically significant differences ($P \leq 0.10$).

	Sectors		Stages		Experience	
	Meat[1] (n=14)	Vegetable[2] (n=6)	Supply [3] (n=13)	Process, retail[4] (n=10)	Yes (n=6)	No (n=17)
*Information sharing**						
Communication management	2.79	2.27	2.62	2.96	**3.28**	**2.41**
Management technology	3.68	3.36	3.54	3.64	3.81	3.51
Relationship management	2.86	2.53	2.56	3.04	3.11	2.47
Public interface management	**3.36**	**2.85**	3.18	3.37	3.61	3.14
*Control actions**						
Process strategy	3.04	2.67	2.85	3.20	3.42	2.85
Process management	2.86	2.41	2.83	2.69	**3.56**	**2.50**
Process technology	2.83	2.77	2.71	3.05	**3.61**	**2.59**
Metrics	2.86	2.40	3.00	2.56	**3.67**	**2.50**
Infrastructure management	3.05	3.22	3.08	3.26	**3.64**	**2.99**
*Robustness**						
Continuation plans in case of lack of facilities	3.14	3.33	3.15	3.40	3.50	3.18
Continuation plans in case of lack of raw materials	3.15	3.33	3.17	3.40	3.17	3.31
Emergency budgets to continue operations	3.15	3.17	**2.83**	**3.40**	**2.67**	**3.25**
*Company's own performance evaluation***	3.21	2.98	3.21	3.14	**3.54**	**3.06**

* Answers were on a scale from 1 (strongly disagree) to 5 (strongly agree).
** Answers were on a scale from 1 (very poor) to 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, retail stage includes processors and wholesale/retail companies.

7. Conclusions and discussion

Information sharing

- 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.

Control actions

- 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.

Robustness

- Robustness seems to be somewhat 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 budgets, companies do not seem to agree to maintain emergency budgets to carry on operations after the occurrence of a security risk.

Security 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 management, 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.

Discussion and impact

The increase in acts of worldwide terrorism has caused food security to become a major concern for the food industry (Dahl, 2007). However, food security did not seem to be a major concern for our respondents. For some of them food security might have been a new issue, or the concept might have not been 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 mistakenly considered as the main guideline and certification

scheme to measure and prevent security risks to the food supply. In this regard, there is gap in creating awareness regarding food security issues.

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 would be difficult to actually detect security risks and prevention and control of the risk could be difficult. This study revealed that companies hardly share information pre and post occurrence of the risk with suppliers and other chain partners. However, as discussed by Dacey (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 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 for external activities such as inspecting suppliers' plants in preventing the risk of intentional contaminations. At the same time, suppliers seem to feel that they are less vulnerable to intentional contaminations. However, individuals or terrorists could use materials such as pesticides, fertilizers, animal feeding substances and irrigation water to intentionally contaminate the food supply (WHO, 2002). In this case intra-partner security assessment seems to be important in preventing intentional risks to the food supply.

The difficulty of anticipating intentional risks, i.e. what kind of intentional risk, when and by whom could it be introduced, is generally used as a plea for chain-wide cooperative work with suppliers, customers and government organizations. Our results however suggest that further security awareness and preparedness programs are needed to ensure that all food supply chains are actually able to act in this way.

8. References

Bryson, S. J., 2005. Terrorism and other public health threats. http://health.yahoo.com/publichealth-bioterrorism/terrorism-and-other-public-health-threats/healthwise--te7507.html.

Closs, D. 2005. Dimensioning a secure supply chain. https://www.ift.org/fooddefense/22-Closs.pdf.

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. http://www.directionsmag.com/article.php?article_id=667&trv=1.

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

Dahl, M. 2007. Food safety- control and oversight, food-borne illness, pesticides and biotechnology, bioterrorism, history and purpose of food safety regulations. http://www.faqs.org/nutrition/Foo-Hea/Food-Safety.html.

FDA, 2003. Risk assessment for food terrorism and other food safety concerns. http://www.doh.state.fl.us/Environment/preparedness/food/resources/rabtact.pdf.

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

Kinsey, J., K. Kaynts and K. Ghosh, 2007. Defending the food supply chain: retail food, foodservice and their wholesale suppliers. The Food Industry Center, University of Minnesota.

NCFPD, 2006. http://www.ncfpd.umn.edu/about/reports/annual_report_2005.pdf.

Sheffi, Y., J.B. Rice, J.M. Fleck and F. Caniato, 2003. Supply chain response to global terrorism: a situation scan. In: Proceedings of EUROMA/POMS Conference, Cernobbio, Lake Como: 5-9.

Takhistov, P. and C. M. Bryant, 2006. Protecting the food supply. J. Food Technology, 34-43.

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

WHO, 2002. Terrorist threats to food: guidance for establishing and strengthening prevention and response systems. WHO, 46 pp., http://www.who.int/foodsafety/publications/general/en/terrorist.pdf.