International Food and Agribusiness Management Review
Volume 14, Issue 5, 2011

Food Risks and Type I & II Errors

William E. Nganje[ⓓ a] and Paul Skilton[b]

[a] *Associate Professor, Morrison School of Management & Agribusiness, Arizona State University, 7171 E. Sonoran Arroyo Mall. Mesa, Arizona, 85212,U.S.A.*

[b] *Assistant Professor, Department of Management, Washington State University-Tri-Cities, 2710 Crimson Way, Richland, Washington, 99354-1671, U.S.A.*

Abstract

The global food supply network is becoming increasing vulnerable to food safety and food defense risks due to failures in prevention and control measures. We develop the idea of control oriented supply chain security management in the context of global food supply networks. We identify a variety of failure points where security systems can produce Type I (false positive) and Type II (false negative) errors that create disruptions, and explain how the use of ex-ante prevention measures can lead to opportunities for continuous reductions in costs and food risks..

Keywords: Food safety, food defense, error based disruption, control oriented supply networks

ⓓCorresponding author: Tel: +1 480.727.1524
Email: William.Nganje@asu.edu
P. Skilton: paul.skilton@tricity.wsu.edu

Introduction

Food processing and distribution involve risk (USDA 2009). Food supply networks are increasingly exposed to food safety and food defense risks partly due to the large volume of shipments from domestic and import sources (USDA AMS 2008; Acheson 2007).[1] However, these risks could be magnified as a result of error based disruptions from Type I and II errors which cause failures in prevention and control measures.

A false positive or Type I disruption occurs when an inspection system incorrectly identifies a threat or a diagnostic system incorrectly identifies a food risk cause, so that a safe product is excluded from the supply chain. Type I disruptions would lead to increased seller's risk, since the seller is exposed to the risk that safe products will be incorrectly devalued. Type I errors are seldom publicly recognized, since they don't affect consumers, but they can have real economic costs to industry. An example of a Type I disruption would be losses incurred when a produce shipment is delayed or destroyed at a Port of Entry (POE) due to a false positive "swab" pathogen test result that could be different from a detailed "culture test", or a producer initiates a mass recall of finished products, rather than a targeted or limited recall, due to ineffective traceability.

A false negative or Type II disruption occurs when a defective product is distributed to the consumer and causes harm that is extensive enough to create market failure (inefficient allocation of goods and services) as a result of the failure to detect the problem or correctly diagnose the cause. Type II disruptions would lead to an increase in buyer's risk, since the buyer experiences the costs associated with the resulting illnesses or deaths. Examples of Type II disruptions are failures to detect accidental contamination from foodborne pathogens, counterfeiting, and adulteration. Some obvious recent examples of Type II disruptions are the melamine adulteration in powder milk powder and the 2006 - *Salmonella* contamination of spinach, both of which led to multiple fatalities. The melamine adulteration episode resulted from an inspection system's failure to detect an intentional, commercially motivated set of actions by some individuals.

The purpose of this study is to assist management, in a business to business (B2B) supply chain that "exceeds" minimal government requirements, to design systems to detect, prevent, and respond to food safety/defense risks in the food supply networks by learning from error based disruptions. While the overarching goal of a control oriented security system is to simultaneously minimize Type I and Type II errors, system improvement can take the form of a reduction in one or both types of error based disruptions or from achievement of cost reductions. We propose that

[1] Food safety can be defined as food system *reliability* – reducing *exposure* to natural hazards, errors, and failures. It is the unintentional contamination of food, which may have dangerous and lingering consequences (Acheson, 2007). Food defense, on the other hand, is system *resiliency* – reducing the *impact* of intentional system attacks from disgruntled employees, terrorists, etc. Chalk (2003) noted that, in the last century, there were several documented cases where pathogenic agents were used to intentionally infect livestock or contaminate food. In September 1984 *Salmonella* food poisoning occurred in The Dalles, near Portland, Oregon when a Rajneeshee group intentionally contaminated restaurant salad bars and caused 751 cases of food poisoning. These individuals were trying to influence a local election. This group also had possession of strains of the causative organism for typhoid fever (Torok, Tauxe, and Wise, 1997). Similar eco-terrorist factions have used plant toxins in Africa (Carus, 1999), anthrax in the UK (Chalk, 2003) and potassium cyanide in Sri Lanka (Cameron, Pate, and Vogel, 2001) to intentionally contaminate food. The term "food protection" is an umbrella term used to define food supply system safety and defense.

control oriented systems differ fundamentally from systems designed to protect against disruptions caused by uncontrollable rare events such as hurricanes, strikes or earthquakes. One way that this difference can be understood is to note that error based disruptions only occur if there are inadequate detection and diagnostic processes intended to control potentially disruptive defects or events (Lee & Wolfe 2003). Once a detection or diagnostic system fails, the normal function of the supply network delivers the defective product to the consumer. This type of problem is thus qualitatively distinct and is further complicated by the complexity of the supply network system.

Error Based Disruptions and Network Complexity

We discuss error based disruption from our understanding of trans-border food supply networks. These networks meet our requirement of including distributed inspection, diagnosis and prevention systems that can be the focus of continuous improvement in control. Trans-border food supply networks are also distinct as they might be easier targets for food terrorism or be subject to multiple risk factors, including smuggling drugs and human trafficking. The first issue we need to address is that of threat. We assume, drawing on the threat-vulnerability-consequence model (Cox 2008; Nganje et al. 2009), that threats are the risk of a food safety outbreak or food terrorism attack arising in any part of the supply network. The kinds of security problems that give rise to threats may be unintentional, as most food borne pathogens contamination appears to be, or intentional, as in adulteration episodes by disgruntled employees or terrorist actions. Food adulteration, whether as a terrorist act or a commercially motivated one, is a principal concern in this kind of security system.

The motivations of the individuals or groups who engage in these behaviors may be political or economic. In either case the intention is to pass unsafe product through the system without detection. This is a significantly important issue because, in adulteration episodes, intentional concealment can be designed to exploit weaknesses in existing security systems. One favorable aspect of intentional behavior is that it often has a point source that, if identified, can lead to the elimination of the threat. Many more error based disruptions will be unintentional, resulting from combinations of events in the food supply network or from normal conditions. Because the cause of these threats can be complex (i.e. have no point source) and because contributing events can be dispersed across the supply network, detection and prevention of unintentional, error based disruptions can be very difficult.

Figure 1 presents a control oriented process map of shipment, inspection, detection, trace, and prevention in the trans-border food supply, identifying error based disruption points and subsequent opportunities for improvement. We discuss the potential failure points in the flow in terms of risk, protection and safety, and then discuss patterns of response that can improve prevention and thus reduce risk while increasing food protection (safety and defense).

The product is shipped and inspected, as shown in the central horizontal axis of Figure 1. Inspection can be performed by a third party (government inspectors at a port of entry), by the carrier, or by the buyer. Every inspection has the potential to generate an error based disruption (Baker & Shuck. 1975; Fortune. 1979). The risk that inspection will generate an error is termed vulnerability in the threat vulnerability and consequence (TVC) model (Cox. 2008). This model will be

extended to include the preventive actions management could implement to mitigate Type I and Type II errors associated with food protection.

Inspection can fail to detect a threat or can incorrectly identify a threat. If a threat is identified, it can either be verified (as in a two stage inspection process) or not. A positive test that is not verified represents a potential false positive or Type I error. If a threat is detected, the shipper and buyer are likely to take action to remove the supposedly unsafe food product from the system, resulting in the loss of the load and, potentially, in the disruption of all products from the source associated with the threat. This is the seller's risk of inspection (Nganje et al. 2009).

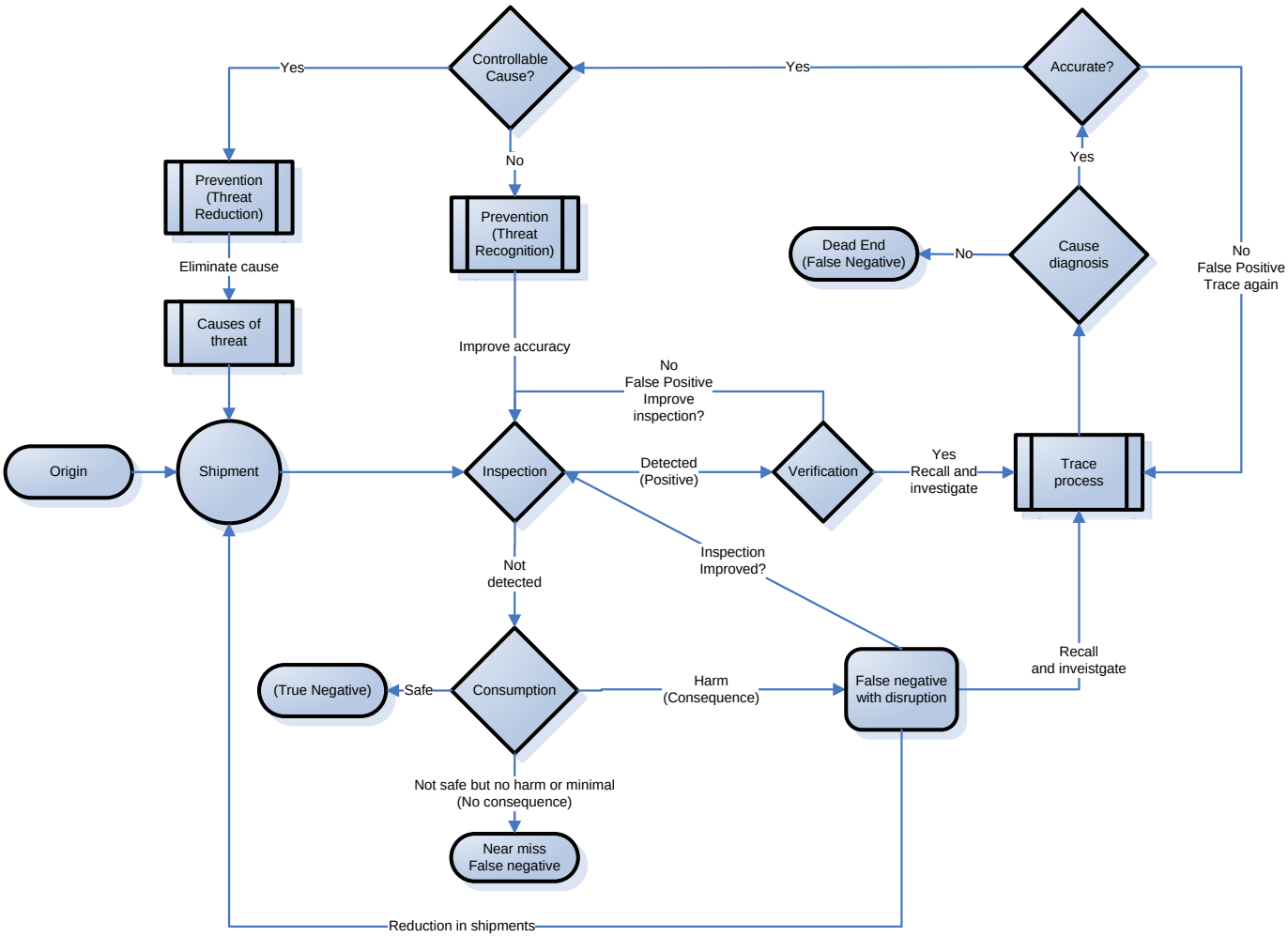

Figure 1. Control oriented supply network security process map

Every Type I error that occurs and is detected in verification represents an opportunity to improve the inspection system (Scazzero & Longnecker 1991; Stewart et al. 2007) in ways that directly reduce cost. Because systems that are overly sensitive will generate a larger number of Type I errors, the resulting opportunities for continuous improvement in inspection are more likely to focus on increasing accuracy and timeliness rather than increasing sensitivity (Baker &

Shuck 1975; Fortune 1979; Scazzero & Longnecker 1991; Stewart et al. 2007). More accurate systems may require more frequent sampling or information sharing between stakeholders and more timely results may require the co-location of testing facilities with inspection stations. Because Type I errors only occur when an inspection system has a specific target, the frequency of these errors also depends on the variety of threats the inspection systems are designed to detect. Most inspections at borders are primarily concerned with agricultural pests and trafficking in people or contraband (Nganje et al. 2009). Because more encompassing, more accurate and more timely inspections presumably increase costs, managers will assess the risk of these disruptions relative to those costs. Because the cost of a false positive may be low (no illness or deaths) relative to other types of disruptions, managers may accept the cost of these disruptions rather than improving the inspection system to prevent false positive results. This may be especially the case when defect rates are very low, since low defect rates may be associated with a greater incidence of Type I errors, such as swab pathogen tests which catch borderline cases.

If a threat is correctly detected during inspection and verified (a true positive), the threat will be removed, and the system may initiate an investigation into the failure to prevent the threat, as we discuss in greater detail below. This should be a normal practice in a continuous improvement orientation in supply chain security (Lee and Whang 2005). In a complex supply network, continuous improvement will require an improvement process that extends to the carrier, the supplier, and any intermediate agents.

If a true threat is not detected in inspection, the potential for a disruption resulting from a Type II detection error is created. For an actual disruption to occur the product must both be consumed and consumption must show recognizable consequences, such as a reported food borne illness or death. In a food supply system, products that are not consumed will not cause illness or deaths. In addition, some defective products may be consumed without actually creating consequences. These scenarios represent 'near misses' – Type II errors that are non-consequential but still represent opportunities for continuous improvement.

We therefore see the consequences of Type II errors as being driven by the risk that an error will be costly – that it will actually have a noticeable effect. These food risks are characterized by class I, II, and III recalls by the Food and Drug Administration (FDA). A Class I recall is a situation in which there is a reasonable probability that the use of or exposure to a contaminated food product will cause serious adverse health consequences or death. A Class II recall is a situation in which the use of or exposure to a contaminated food product may cause temporary or medically reversible adverse health consequences or where the probability of serious adverse health consequences is remote. A Class III recall is a situation in which use of or exposure to a contaminated food product is not likely to cause adverse health consequences (USDA-FDA 2009).

Based on studies of accidents in other complex systems (Perrow 1999; Sagan 1993; Weick & Roberts 1993) it is very possible that lapses in inspection programs represent the majority of Type II errors in food supply systems. This is because the observed rate of disruptions is a function of the effectiveness of inspections[2], the consumption rate and the use of alternative risk re-

[2] FDA operations inspect about 1% of the imported foods it regulates, down from 8% in 1992 when imports were far less prevalent (Schmidt, 2007).

duction strategies (e.g., cooking the product well). If the severity of Type II errors is underestimated it leads to inaccurate assessments of systemic risk which, in turn, influences decision processes concerning internal and external security policy (Cox 2008; Nganje et al. 2009; Verduzco, Villalobos & Vega 2001; Voss et al. 2009; Voss, Whipple & Closs 2009). Inaccurate assessment of Type II severity is a potential major failing in many food supply chain security systems, with frequent occurrences of food recalls resulting from the system failing to identify contaminated products.

The most extreme consequence of a Type II disruption in the food supply system is that one or more consumers gets sick or dies. Product recalls and supply disruptions are the almost inevitable consequences of Type II disruptions. Far more than Type I disruptions, Type II disruptions lead to calls to improve inspection systems. Unlike inspection improvement efforts resulting from Type I disruptions, efforts following Type II disruptions nearly always involve increasing the sensitivity and scope of inspections and policy. Once supply chains, brands and firm survival are threatened by a Type II disruption, managers become much less concerned with the cost of inspection and prevention improvements. The need for inspection to be seen as taking action can create new occasions for increased seller's risk, since the actions taken will not necessarily improve diagnosis, inspection or prevention (Verduzco, Villalobos & Vega 2001). For example, the Bioterrorism Act of 2004 only requires improvements in record keeping that improve traceability, without requiring changes in inspection or prevention methods. Improvements to traceability may create opportunities for improved protection and safety, but these opportunities must be exploited to achieve actual improvements. This risk of ineffective controls legitimizes our emphasis on cost, since it provides a basis for making choices between investments in inspection, diagnosis and prevention.

Investments following Type II disruptions resulting from inspection errors can be aimed at improving inspection or at diagnosing causes, thereby enabling prevention oriented investments aimed at reducing threats. Diagnostic processes, which are usually called traceability processes, have the potential to fail, which we call diagnostic risk. Diagnostic systems can produce false positives (Type I diagnostic error) and false negatives (Type II diagnostic error), by providing timely and targeted recalls when there is a known food borne disease outbreak.

How likely a Type II diagnostic error is to occur depends in large part on the structure of the supply network. Because traceability involves identifying and verifying the components and chronology of events in all steps of a process chain, Skilton and Robinson (2009) propose that its effectiveness is a function of the level of complexity in the supply network on one hand and the degree of tight coupling within the supply network on the other. In systems where supply networks are relatively simple and tightly coupled through integrated process structures and coordinated information exchange, traceability is a relatively straightforward process. We suspect that systems with these characteristics, which we associate with branded goods and processed food, are also likely to have relatively low levels of diagnostic risk. Although Pomonarov and Holcomb (2009) argue that the risk of disruption is greatest for such firms, we suggest that, because the consequences of disruption are perceived as greater, these firms are more likely to have systems that allow accurate diagnosis of errors. These food supply networks will be able to quickly trace the causes of disruptions. As network complexity increases, diagnostic risk will tend to increase, particularly if complexity reduces the timeliness and accuracy of information flows, or

compliance with security measures. Because traceability and diagnosis will be less effective, fewer opportunities for improvement will emerge. Supply chain managers will be confronted with a need to trade-off the benefits of network complexity against the costs of tight coupling and information coordination which enable rapid traces and accurate diagnosis.

Diagnostic risk will be greatest in supply networks that are loosely coupled and complex (Skilton & Robinson 2009). In these networks, which are relatively common in the commodity sectors of the food supply system, it can be very difficult to accurately diagnose the causes of disruptions. Because networks are complex and entangled, inaccurate diagnosis can create Type I diagnostic errors that compound the cost of the initial disruption. One example of a Type I disruption in tracing was the incorrect association of tomatoes with *salmonella* contamination in 2007. This false positive diagnosis led to a nationwide tomato recall that cost growers and packers more than $30 million (USDA 2008).

Although the risk of diagnostic errors is greater in complex, loosely coupled networks, security efforts are often substantially lower in these networks because the participants have significantly lower investments in brand and reputation to protect, reducing the perceived severity of failures. These factors combine to make this the sector most exposed to consequential error based disruptions. Reduced prevention and inspection increase the likelihood of Type II errors, and a loose network structure will impede traceability and improvement efforts. This environment also invites intentional food contamination. While food terrorist actions have been infrequent (Chalk 2003; Engel 2000), intentional adulteration for commercial reasons was the source of the Chinese infant formula melamine poisoning event (Chao 2007) and is probably more common than is generally recognized. The threat of supplier opportunism should be as much a consideration in supply chain security as terrorism is (Roth et al. 2007; Voss et al. 2009).

When an accurate trace is carried out and the source or agents are identified, the system has an opportunity to improve prevention. In the food supply network, preventive security measures include supplier selection standards, supplier development and certification, facility design and protection processes, employee screening and training, shipment tracking, process integration and process monitoring (Closs & McFarrell 2004; Lee & Whang 2005; Roth et al. 2007; Voss, Whipple & Closs 2009; Williams, Lueg & May 2008). The presence of known inspection processes may serve to prevent some kinds of threats from being deployed (Chao 2007), but tests that are too narrow may invite other specific kinds of threats. Supply chain security personnel should remain aware that intentional threats in particular will tend to adapt to changes in security systems (Chalk 2003; Cox 2008). When intentional disruptions occur and can be traced, managers are faced with the dubious luxury of having an identifiable point source of a set of actors who can be prosecuted or whose access to the system can be removed.

Changes to preventive measures often follow from successful traces in response to Type II disruptions at the moment when cost-based resistance is least and the perception of risk is greatest. They are often adopted as governmental initiatives (e.g., U.S. Customs initiatives such as C-TPAT and advanced electronic notice of shipping manifests) or industry initiatives (California Leafy Greens Marketing Agreement, ISO 28000 standards addressing supply chain security; the International Maritime Organization's International Ship and Port Facility Security Code). Governmental and industry level initiatives have the advantage of leveling the playing field in terms

of implementation costs, but may not provide enough incentives for all parties along the supply chain to fully adopt food risk mitigation strategies (e.g., smaller firms may be given more time to implement a policy or acquire more resources). Strong central players in supply networks can complement federal efforts by imposing their own more stringent standards on producers and distributors, such as Wal-Mart's sustainability and food safety initiatives (Rosenbloom 2008). In the next section we discuss a comprehensive detection, prevention, and response framework that managers and policy makers could use to mitigate food risks and error based disruptions.

A Control Oriented Framework and Reduction of Type I and Type II Errors

A comprehensive detection, prevention, and response framework would have four major components: 1) to identify the roles and synergies of multiple stakeholders, 2) to establish procedures to assess threats, vulnerability, and consequences along the food supply chain, 3) to identify incentives for management to adopt and implement controls oriented risk mitigation plans and 4) to develop a feedback system for response and continuous improvement.

A major challenge with having multiple stakeholders is how to identify synergies which may lead to developing consistent risk mitigation policies. One approach may be to use Scenario Method Analysis, a qualitative approach for determining drivers and dependent variables.[3] This would provide a framework to avoid duplication but yet facilitate validation so that the cost and risks associated with Type I and II errors are minimal.

Figure 2 describes a conceptual framework to address the last three components of the threat-vulnerability-consequence model (Cox 2008; Nganje et al. 2009). The process map visualized in Figure 1 and described above contains the elements necessary for a theoretical framework of control oriented management in supply chain security systems. This framework defines the varieties of risk inherent in security systems and relates them to the investments and commitments necessary to achieve a balance between security costs and benefits. Figure 2 provides a systemic view of costs and risks and the relationships between them. How managers respond to opportunities for controlling threats and costs governs the evolution of supply chain security systems. Figure 2 provides a road map for the definitions and propositions that follow.

Beginning in the upper left corner of the figure, it seems self-evident that threats have causes (+ indication). In most security oriented studies, the causes of threats are treated purely as exogenous. As shown in Figure 2, in a control oriented framework, this is not the case. The causes of

[3] *Scenario Method Analysis* provides a qualitative approach to identify influence and dependent factors for the short-run (direct effects) and long-run (indirect effects with second- and third-order interaction) to enable all stakeholders determine what synergies and contributions in mitigating food risks should be considered. The Micmac Scenario Method is based on the formulation by Godet (1987). The analysis involves developing a database of important variables/factors from existing literature or survey, determining the relationship between factors (with 0 = no relationship and 3 = very strong impact), analyzing and classifying variables into four major quadrants: strong dependent and influence variables, strong dependent and weak influence variables, weak dependent and strong influence variables, and weak dependent and influence variables. The method derives second- and third-order interactions between factors from three environments: *internal firm environment, external policy environment, and the competitive market environment.* The *MicMac Software* is used to perform the analysis.

threat may initially be poorly understood, but an important goal of a control oriented system should be to understand causes of contamination in order to eliminate or control them (Bohn 1994; Lee & Whang 2005). Improved knowledge of control factors achieved through diagnostic processes often results in preventive measures, to which we will return at the conclusion of this section.

We have defined threats as the perceived risk of a defect or attack in a specified supply chain. We define vulnerability as the risk of errors in detection systems. Threats can arise at any point in a supply chain. For convenience we will conceptualize threats to be associated with shipments, but threats could equally be associated with facilities or personnel. The whole purpose of control oriented supply chain security systems is to estimate and control threats. This means that threats must be perceived, since a threat that is not anticipated cannot be estimated, controlled or defended against.

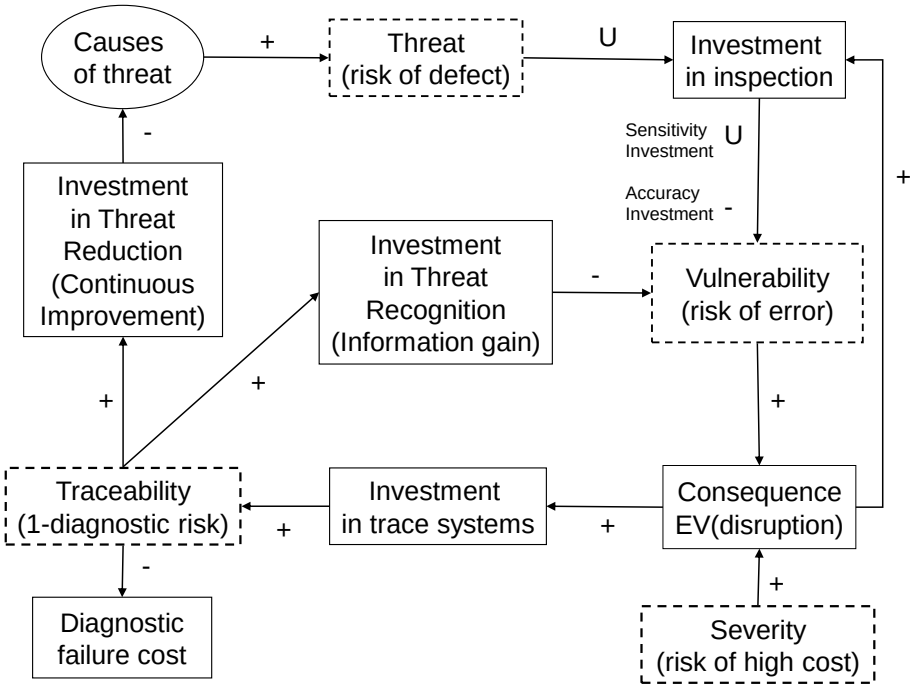

Figure 2. Control oriented supply network security conceptual model

Proposition 1 The relationship between threat, vulnerability, and investment in detection will be non-linear but positive, so that investment will grow less quickly as threats increase.

Arguments for Proposition 1. We assume, as many others have, that as threats increase, participants in supply chains will increase their investments in systems designed to detect defects and attacks before they reach the markets that are their targets. This is in contrast to protection oriented supply chain security systems that invest in hardening targets or creating back-up systems. In control oriented supply chain security systems, these investments relate primarily to inspec-

tion systems. Such investments can improve the sensitivity of inspections, the accuracy of inspections or both. We further propose that there are decreasing returns to detection systems such that, as the probability of defects or attacks increases, improvements in detection resulting from additional investments will diminish. When the threat is low, the benefits of additional investments in inspection systems (such as frequent sampling) will be constrained by the likelihood that greater sensitivity will increase the Type 1 error rate. As threats increase, benefits from additional investment will initially rise, and then plateau. Highly probable defects will be easier to detect with lower sampling rates and lower levels of investment, so that the form of the relationship between threat and investment in detection is likely to take an inverted U shape (presented in Figure 2). This could be illustrated best with the knowledge that as we increase investment in sampling and testing for pathogens we could produce both Type I and Type II errors. Investing in a more sensitive inspection system will decrease the likelihood of Type II errors while potentially increasing the likelihood of Type I errors. The real question here is whether investing in detection systems increases the net risk of combined Type I and Type II errors. We would argue that, in control oriented systems, investments to improve accuracy will decrease Type II errors without increasing Type I errors because the efficiency of all control units will be improved. On the other hand, investments in the detection of contamination will increase Type 1 errors while reducing Type 2.

Proposition 2. Vulnerability is positively related to consequence.

Arguments for Proposition 2. Consequences, which we define as the expected cost of disruptions, are positively related to vulnerability. The more vulnerable a security system is, the more likely it is that an error will occur resulting in a system disruption. How consequential a disruption is depends on the ways the product is used and by whom. A market failure resulting from a Type 1 error that leads a producer to withdraw a product that is actually safe could be as consequential as a complete market failure resulting from a terrorist poisoning a food supply.

Proposition 3. Consequence is positively related to investments in detection systems.

Arguments for Proposition 3. As a practical matter we would expect greater consequences, realized or perceived, to be positively related to investments in detection systems. Unlike the relationship between threats and investments in detection systems, we think that this relationship will be linear. Where consequences are very large, managers will take corresponding steps to invest in and improve detection. This is a central tenet of research on high reliability systems (Sagan 1996; Weick & Roberts 1993). Finally, consequences need not be realized to influence behavior. The perception that consequences will be high can lead to action.

Once we move beyond consequences, the remainder of the model deals with prevention (Nganje et al. 2009; Lee & Whang 2005). One of the principle contributions of this article is the inclusion of diagnostic systems designed to trace the root causes of disruptions. This is a key element in a prevention and control orientation generally. Only by diagnosing the causes of errors can we close the loop and achieve a control oriented system of supply chain security. The framework can also serve as a launching point for empirical research. Several of our propositions should be easily tested with the right empirical data. Finding support for this or an alternative model of these relationships will have important implications for practice in control oriented supply chain

security management. We think this is an important opportunity because most supply chain security managers are first and foremost supply chain managers. They will thus have a natural interest not only in achieving control of supply chain security, but also in finding ways to simultaneously mitigate threat and control the costs of errors.

Managerial Implications and Feedback for Continuous Improvement

Error based disruptions and risks that managers have opportunities to control are probably the most common types of disruption in food supply networks. Because food risks from an individual firm are relatively infrequent, managers are often reluctant to commit to permanent overhead costs to prevent them. As with uncontrollable disruptions, however, the consequences of allowing disruptions to take place may be much greater than anticipated. Not only can revenue flows be interrupted, often for long periods, but the value of brands can be seriously impaired when consumers become sick or die from food hazards.

In this paper we have pointed out a number of factors that make perceptions of the risk of error based disruptions inaccurate. First, Type I disruptions are often not considered as failures of the security system, when in fact they are. Shipments that are delayed, blocked or recalled when they are actually safe may be the major controllable cost in supply network security. This is an area where costs arise from compliance with regulations that are too sensitive or where tests are too sensitive or both. Type I errors represent an important opportunity for continuous improvement in inspection systems, an area that both managers and scholars may have overlooked for too long.

Second, the perceptions of risks relating to Type II disruptions may be systematically underestimated if their severity is characterized by a high proportion of near misses. There is a clear opportunity for future research to try to quantify and model these unseen costs and risks.
It is also important to recognize, as we have, that not all supply networks are exposed to the same levels of security risk. Highly integrated supply networks organized to include structured distributed detection and diagnosis processes, sustained relationships and extensive partner monitoring are much less likely to be exposed to error based disruptions. When error based disruptions do strike these networks they are more likely to be Type I events that do not threaten brand or production systems. Supply networks that rely on loosely coupled commodity trading (with complex tracing situations) are much more exposed to both Type I and Type II disruptions, and should therefore be the focus of management and regulatory agencies. Management wishing to improve control over their supply chain security should seriously consider abandoning this type of network in favor of a relatively simple, but more highly integrated structure (e.g., production with a contract/food protection environment like the Leafy Greens system). One important reason to do this is because it improves traceability, which is the key to improving the preventive measures that are necessary to achieve control in supply network security.

Management should address these issues related to information and network complexity to minimize errors and costs. Information systems designed for linear, tightly coupled networks will not meet the challenges of complex supply networks. Different network structures have to address additional problems such as preserving information through transformation processes or the comingling of shipments that simply don't occur in simple, tightly coupled networks. In tightly

coupled networks, a powerful central player can make traceability systems much more effective, but only at a high cost in terms of system resources, data quality and the opportunity costs of committing to a smaller supplier base for any product. While we think that reconfiguring complex loosely coupled networks toward this more tightly coupled model would improve traceability and security, it might come at a high economic cost. This is the risk equation that many supply networks face, and thus far the tendency has been to maintain the structure and treat security failures as an acceptable risk. One area where the rewards of future research may be great will be the study of real time information systems (electronic barcodes and radio frequency identification devices) and the ways that they can improve accuracy. There is some hope that real time information can improve control of Type I disruptions and help reduce the rate of near misses in Type II disruptions.

There have been proposals that trust and embeddedness in networks that value quality and transparency can enhance traceability at a relatively lower cost (Roth et al. 2007; Skilton & Robinson 2009). Continuous improvement in supplier relationships to increase trust and transparency (Lamming, Caldwell & Harrison 2004; Lamming et al. 2001) has to be accompanied by continuous attention to and recertification of information flows and integrated processes. While trust and transparency may reduce the cost of inspection and prevention, they are not a substitute for such measures. Because trust and transparency can reduce perceptions of risk without actually reducing it, managers need to follow Ronald Reagan's security dictum: 'Trust, but verify'.

Although we have emphasized the ways in which current systems can fail, we have done so in the spirit of continuous improvement. We think that a continuous improvement approach (Lee and Whang 2005), combined with a security orientation (Autry & Bobbit 2009) that embraces a willingness to make data based decisions about the cost trade-offs of controlling error based disruptions will be central to more successful supply chain security management. Only by achieving an accurate assessment of total risks can supply chain managers make informed decisions that lead to the least costly, most effective, control oriented supply chain security systems.

References

Acheson, David. 2007. PBS News Hour. http://www.pbs.org/newshour/bb/health/jan-june07/foodacheson_06-08.htmlen (accessed Feb. 16th 2010).

Baker, Edward M., and John P. Schuck. 1975. Theoretical Note - Use of Signal Detection Theory to Clarify Problems of Evaluating Performance in Industry. *Organizational Behavior and Human Performance* 13(3): 307-317.

Bohn, Roger E. 1994. Measuring and Managing Technological Knowledge. *Sloan Management Review* 36(1):61-73.

Cameron, G., J. Pate, and K.M. Vogel. 2001. Planting fear. How Real is the Threat of Agricultural Terrorism? *Bulletin of the Atomic Scientists* 57 (5):38-44.

Carus, W.S. 1999. Bioterrorism and Biocrimes: The Illicit Use of Biological Agents in the 20th Century. Center for Counter-Proliferation Research, National Defense University, Washington, DC.

Chalk, P. 2003. The Bio-terrorist Threat to Agricultural Livestock and Produce. CT-213 Testimony, presented before the Government Affairs Committee of the United States Senate, 19 November.

Chao, L. 2008. China Bolsters Dairy Supply Oversight in Effort to Rebound from Scandal. *The Wall Street Journal*, October 7: A19.

Closs, D.J. and E. F. McGarrell, E.F. 2004. Enhancing security throughout the supply chain. *Special Report Series, IBM Center for The Business of Government*, available at: www.businessofgovernment.org .

Closs, D.J., C. Speier, J. Whipple and M. D. Voss. 2008. A framework for protecting your supply chain. *Supply Chain Management Review* 12 (2): 38-45.

Cox, L. A. Jr. 2008. Some Limitations of "Risk = Threat × Vulnerability × Consequence" for Risk Analysis of Terrorist Attacks. *Risk Analysis*, 28(6)1749-1761(13).

Engel, Eduardo M.R.A. 2000. Poisoned Grapes, Mad Cows and Protectionism, No 76, Documentos de Trabajo, Centro de Economía Aplicada, Universidad de Chile.

Fortune, Bill D. 1979. The Effects of Signal Probability on Inspection Accuracy in a Microscopic Inspection Task: An Experimental Investigation. *Academy of Management Journal* 22(1):118.

Godet, Michael. 1987. Scenarios and Strategic Management, Butterworth, London.

Lee, H.L. and M. L. Wolfe. 2003. "Supply chain security without tears", *Supply Chain Management Review* 7(1): 12-20.

Lee, Hau L and Seungjin Whang. 2005. Higher supply chain security with lower cost: Lessons from total quality management. *International Journal of Production Economics* 96(3): 289-300.

Nganje, William, Timothy Richards, Jesus Bravo, Na Hu, Albert Kagan, Ram Acharya, and Mark Edwards, 2009. Food Safety and Defense Risks in U.S.-Mexico Produce Trade, *Choices: The Magazine of Food Farm and Resource Issues* 24(2) 16-20. http://www.choicesmagazine.org/magazine/pdf/block_31.pdf, accessed Feb. 16, 2010.

Perrow, C. 1999. *Normal Accidents: Living with High Risk Technologies*, Princeton University Press, Princeton, NJ.

Ponomarov, Serhiy Y. and Mary C. Holcomb. 2009. Understanding the concept of supply chain resilience. *International Journal of Logistics Management* 20(1): 124-143.

Rosenbloom, S. 2008. Wal-Mart to Toughen Standards. *The New York Times*, Oct. 22, B1.

Roth, A.V., A.A. Tsay, M.E. Pullman and J.V. Gray. 2008. Unraveling the Food Supply Chain: Strategic Insights from China and the 2007 Recalls. *Journal of Supply Chain Management* (44):22-40.

Sagan, S.D. 1993. *The Limits of Safety: Organizations, Accidents and Nuclear Weapons*, Princeton University Press, Princeton, NJ.

Scazzero, Joseph A., and Longnecker, Clinton O. 1991. The Illusion of Quality: Controlling Subjective Inspection. *Journal of Applied Business Research* 7(1): 52.

Schmidt, J. 2007. U.S. Food Imports Outrun FDA Resources. *USA Today*, March 18.

Skilton, P., and J. Robinson. 2009. Traceability and normal accident theory: How does supply network complexity influence the traceability of adverse events? *Journal of Supply Chain Management* 45(3): 40-53.

Stewart, K., J. Carr, C. Brandt, and M. McHenry. 2007. An Evaluation Of The Conservative Dual-Criterion Method For Teaching University Students To Visually Inspect AB-Design Graphs. *Journal of Applied Behavior Analysis* 40(4): 713-8.

Torok, T., R. V. Tauxe, and R. R. Wise. 1997. A Large Community Outbreak of Salmonella Caused by Intentional Contamination of Restaurant Salad Bars. *The Journal of the American Medical Association* 278(5), 389-395.

(USDA) U.S. Food and Drug Administration. 2008. Salmonella Saintpaul Outbreak, http://www.fda.gov/oc/opacom/hottopics/tomatoes.html, Accessed October 16, 2008.

US Food and Drug Administration (FDA). 2009. *Safety*. Retrieved on September 13, 2010 from http://www.fda.gov/Safety/Recalls/ucm165546.htm.

Verduzco, Adan , J. Rene Villalobos, and Benjamin Vega. 2001. Information-based inspection allocation for real-time inspection systems. *Journal of Manufacturing Systems* 20, no. 1, (January 1): 13-22.

Voss, M., D. Closs, R. Calantone, O. Helferich, and C. Speier. 2009. The Role of Security In The Food Supplier Selection Decision. *Journal of Business Logistics* 30, no. 1(Jan. 1): 127-9.

Voss, M., J. Whipple, and D. Closs. 2009. The Role of Strategic Security: Internal and External Security Measures with Security Performance Implications. *Transportation Journal* 48, no. 2, (April 1): 5-23.

Weick, K.E., and K.H. Roberts. 1993. Collective Mind in Organizations: Heedful Interrelating on. *Administrative Science Quarterly* 38(3):357.

Williams, Zachary, Jason E Lueg and Stephen A. LeMay. 2008. Supply chain security: an overview and research agenda. *International Journal of Logistics Management* 19(2): 254-281.

