Prepared for Bioterrorism Events? A Study of the Grain and Oilseed Sector

Eric J. Wailes, Rita Carreira, Diana M. Danforth and Vivek Nemane

Department of Agricultural Economics and Agribusiness
University of Arkansas, Fayetteville
Division of Agriculture

Poster prepared for presentation at the Agricultural & Applied Economics Association's 2011 AAEA & NAREA Joint Annual Meeting, Pittsburgh, Pennsylvania, July 24-26, 2011

Prepared for Bioterrorism Events? A Study of the Grain and Oilseed Sector

Eric J. Wailes, Rita Carreira, Diana M. Danforth and Vivek Nemane
Department of Agricultural Economics and Agribusiness, University of Arkansas, Division of Agriculture

Problem and Objectives

One of the most crucial problems facing the U.S. economy is the possibility of a terrorist attack on its food sector. The implications can be profound for its stakeholders, who are highly dependent on this sector for their economic livelihood as well as their food supplies.

The U.S. Bioterrorism Act of 2002 was enacted to improve the ability of the United States to prevent, prepare for and respond to bioterrorism and other public health emergencies. One of the important features of the U.S. Bioterrorism Act of 2002 is its emphasis on prevention, a change from prior legislation that focused on punishments after an incidence had occurred. The U.S. Bioterrorism Act does not address food safety issues in general; its focus is to prevent intentional contamination.

The objective of this study was to assess the preparedness to potential bioterrorism in the grain and oilseed sector based on facility security expenditures and history of security breaches. The study was conducted as a research activity under the multistate project NC-1016 "Economic Assessment of Changes in Trade Arrangements, Bio-terrorism Threats and Renewable Fuels Requirements on the U.S. Grain and Oilseed Sector."

In addition to assessing preparedness, the study investigated the relationship between adoption of security measures and breaches in facility security. Finally the study documents, for a small sample, the extent to which grain and oilseed facilities appear to be following regulations that implement the U.S. Bioterrorism Act.

Government agencies have promulgated regulations to implement the U.S. Bioterrorism Act but it is often difficult to identify actual constraints in the implementation. A compliance guide prepared by the National Grain and Feed Association describes the regulations applicable to grain and oilseed facilities as follows:

A. Registration of food processors: Domestic and foreign facilities (and their U.S. agents) that manufacture, process, pack or hold food for human or animal consumption in the U.S. were to be registered with the FDA. According to the registration requirement, all establishments at which food is manufactured or processed, packed or held are required to be registered. The "collecting facilities" are described as the facilities that store or hold food, such as silos or grain elevators; hence such a facility must be registered with the FDA because food is held by the facility. Facility registration is required for grain elevators, feed mills, flour mills, corn and oilseed processors, pet food manufacturers, renderers and others. The information mainly comprises of the description of food products including their brand names and general food categories along with the facility address and the contact information.

B. Maintenance of records: Facilities are required to establish and maintain records containing information that is „reasonably available". The information includes

a) Immediate previous source (the seller)
b) Immediate subsequent recipient (the buyer)
c) The dates of inbound and outbound shipments
d) Type and quantity of agricultural commodity received and shipped
e) Identity and contact information of the transporter

Analytical Framework

The facility maximizes its expected profit as described in:

(1) $\max E(\pi_i) = E[P y_i (- C_i (Y_i) - A_i (m_{1i}, \ldots, m_{ni}) S_i - p_i (m_{1i}, \ldots, m_{ni}) L_i]$

where π_i is profit of facility i, P is output price and C_i represents the facility's production cost structure which depends on output level. We make the simplifying assumption that security costs are separable from production costs. The annual cost per unit of storage (S_i) of implementing preventative security measures $m_{1i}, \ldots, m_{ni}$, depends on the measures themselves and is denoted by A_i. We divide the expenditure in security measures by the size of the facility to eliminate the effect of size on cost. A facility that engages in preventative measures will face security costs of $A_i(m_{1i}, \ldots, m_{ni}) S_i$.

The cost of implementing the security measures is modeled as a linear regression, that is,

(2) $A_i = \mathbf{X_i}\boldsymbol{\alpha} + \varepsilon_i$, ε_i *is iid* $N(0,\sigma^2)$

In this regression, $\mathbf{X_i} = [1 \; m_{1i} \ldots m_{ni}]$ where $\mathbf{X_i}$ represents the row vector of dimension 1 x (n + 1) that represents the security measures at facility i and $\boldsymbol{\alpha}$ is the (n + 1) x 1 column vector of parameters associated with the explanatory variables. The intercept parameter represents a fixed cost of securing a facility, while the slope parameters are estimates of the cost associated with each measure.

The probability of a disruptive event happening in facility i is given by p_i, which is also a function of the security measures implemented at the facility. Thus the last component in the expected profit function $p_i(m_1, \ldots, m_n) L_i$, is the expected monetary loss due to a disruptive event that takes place in the facility. We model p_i as a logit regression such that,

(3) $\text{logit}(p_i) = \mathbf{X_i}\boldsymbol{\beta}$,

where $\boldsymbol{\beta}$ denotes the vector of parameters that we wish to estimate. A negative sign of the parameter indicates that facilities that adopted the measure are associated with smaller incidence of disruptive events. Profit maximization is achieved by selecting the optimal level of output and security measures to implement.

Study Framework

A questionnaire was sent to all grain and oilseed processors, elevators, feed mills and feed stores in Arkansas in order to obtain information regarding the existence and response to bioterrorism. From the population of 258 facilities, a total of 46 responded. Table 1 shows the response distribution of facilities by type.

Table 1. Facilities by type

Facility Type	Number	Percent
Country elevator	18	39.1
River elevator	3	6.5
Feed mill	3	6.5
Rice mill	3	6.5
Soybean processor	3	6.5
Seed facility	6	13.0
Feed store	10	21.7
Total	46	100.0

The most common security breaches reported by facilities were minor theft, minor vandalism and unauthorized entry (Table 2). None of the facilities reported intentional contamination, transport sabotage or bomb threats.

Table 2. Percent of facilities who reported security breaches over the last 5 years (2006-2010)

Type of Event	% with one or more events	N
Unauthorized entry	27	45
Minor vandalism ($1-3,000)	36	45
Major vandalism ($3,001 or more)	2	42
Intentional contamination of the grain	0	45
Sabotage of the transport infrastructure	0	45
Minor theft ($1-3,000)	50	44
Major theft ($3,001 or more)	13	45
Bomb threat	0	45

When asked how current security measures compare to those in place before 2002, 50% of facilities reported better security. Facility surveillance systems and on-line security protection were implemented by over 20% of facilities after 2002 (Table 3). Still, only slightly over half of facilities reported having a surveillance system. Only a third of facilities had controlled gate access, perimeter fencing, or quarantine procedures in place. Average annual expenditure per facility for security was $11,292.

Table 3. Percent of with security measures by implementation date

		Yes		
Plant Security Measures	No	Before 2002	After 2002	N
Record-keeping system that tracks commodities	12.2	70.7	17.1	41
Disaster training	48.8	32.6	18.6	43
Quarantine procedures	67.5	27.5	5.0	40
Coordination agreement between facility and first responder authorities	54.8	30.9	14.3	42
Security lighting	0.0	91.1	8.9	45
Perimeter fencing	69.1	21.4	9.5	42
Controlled gate access	69.0	19.1	11.9	42
Facility surveillance system (alarms, video, etc.)	48.8	25.6	25.6	43
Employees are trained to report suspicious behavior to management	7.0	74.4	18.6	43
Computers and on-line security protection	50.0	28.6	21.4	42
Barriers to prevent access to ladders, catwalks, and other entry points	53.6	41.5	4.9	41

Over three quarters of facilities tested every load delivered on receipt, both before and after 2002 (Table 4).

Table 4. Percent of facilities with inbound commodity testing

	Test every load delivered upon receipt	Test over 50% of loads delivered	Test less than 50% of loads delivered	N
Before 2002	76.5	5.9	17.6	34
Since 2002	77.8	5.5	16.7	36

Results

Few Pearson correlation coefficients between the adoption of security measures and security breaches were statistically significant. We found that some security measures were correlated with each other. In the estimation of equation 2 which relates security spending per unit of storage capacity to the preventative measures implemented at a facility, we found that only the amount of product being tested can explain the variation of spending around its mean. The R-squared of this regression is 0.4793 (Table 5). The parameter estimates indicate that, on average, facilities that test 100% of their product spend $19,977 less per thousand of bushels of storage capacity on security than facilities that test less than 50% of product; and facilities that test less than 100% but more than 50% of their product spend $19,928 less per thousand of bushels of storage capacity on security than facilities that test less than 50% of product.

Equation 3 of our model posited that the probability of security breach outcomes are a function of the security measures in place at a facility. However, this model was not well supported by our data. None of the logistic regression models that we estimated indicated the presence of such an effect. These results are not surprising as the Pearson correlation coefficients of the security events and the security measures were not statistically significant.

Table 5. OLS Parameter Estimates of Security Spending

Variable	Parameter estimate	Standard Error	p-value
Intercept (Test < 50%)	20,002	4,170	<.0001
Test 100%	-19,977	4,356	0.0001
Test >50%	-19,928	5,897	0.0026

Conclusions

This study found that facilities have limited investment and expenditures on facility security. Our failure to establish a connection between security practices and breaches may indicate that facility decision makers have different preference functions for risk. The adoption rates and the variety of comments received from respondents indicates that a full understanding and/or enforcement regarding implementation of the U.S. Bioterrorism Act of 2002 are lacking.

References

Public Health Security and Bioterrorism Preparedness and Response Act of 2002, Pub. L. No. 107-188, 116 stat. 594

Randall C. Gordon and David A. Fairfield, *National Grain and Feed Association, FDA'S Bioterrorism Recordkeeping Regulations, A Compliance Guide for Grain Elevators, Feed Manufacturers, Feed Dealers, Integrators, Grain Processors and Transporters (April, 2006).*

Vivek Nemane. 2011. Food and Agricultural Security Strategy and its Implementation under the Public Health Security and Bioterrorism Preparedness and Response Act of 2002. LL.M. Thesis, Agricultural Law, University of Arkansas.

This research was supported by a grant from the Arkansas Agricultural Experiment Station, Division of Agriculture, University of Arkansas.