Providing Security to Food Transportation Systems without Compromising Productivity

DR. ALLAN ERERA
GEORGIA TECH

We're going to move onto the next presentation in this session, which will be given by me. The next 4 talks in the session will be given by academic researchers, and thus we're going to shift the focus a bit now into research perspectives in this area. As I mentioned earlier, I'm a professor here at Georgia Tech in the School of Industrial and Systems Engineering, and I'm affiliated with The Logistics Institute (TLI). Our primary research focus, I would say, is the development of decision technology to improve decision-making for logistics and freight transportation processes.

The title of my talk today is “Providing Security to Food Transportation Systems without Compromising Productivity”, and I want to say right away that I don't have all the answers to this question. I do think, however, and I agree with Mr. Sims on this point, that it's very important when we look at security related problems that we keep in mind the productivity implications on the systems that we are securing. So I want to talk to you briefly about an overview of the types of research themes that we address in this area and ones that I think deserve additional consideration going forward. The 3 major themes that I want to cover today are the following:

First, I think it's first very important as researchers with the National Center for Food Protection and Defense to understand the security vulnerabilities and concerns of the freight transportation providers to the food industry. Additionally, and this is not mentioned specifically on this slide, is that we also would like to understand what companies are doing to provide supply chain security, hopefully in a productive and cost efficient manner. What are best practices in this area? I think the next presentation, by Dr. David Closs, will be providing more detail on our effort there, but I will also spend some time on this.

The second important theme in our research agenda is that we believe it's critically important to quantify the productivity impact of supply chain security initiatives. I'll give you a number of reasons for this when I get to this component of the talk. Often this step does require research, and I'll hopefully be able to illustrate that a bit with some simple examples. Lastly, the final theme of our research is that terrorist-related disruptions to supply chains are just one source of potential business disruption. We believe that there is a need to systematically investigate methodologies for designing and controlling secure, cost-effective, and resilient supply chain systems, where resiliency may be with respect to any sort of disruption. So these are the three themes that I want to go through today and I'll illustrate some of the things that we're doing, especially for the first 2, with some simple examples.

First, let's talk briefly about domestic food supply chain systems. Now while I put the word “food” up there, most supply chains for all sorts of products look very similar. You may have a tier of suppliers that serve a manufacturing facility or production facility of some sort; these facilities may serve distribution facilities which eventually serve retailer outlets, which in the case of food also include restaurant retail facilities which serve the end consumer. Additionally, I've drawn in black arrows to represent the flow of goods through the system. If you look in the reverse direction, and I know it's hard to see the arrows, but the information flow typically flows backwards along this network. There may be additional suppliers to your suppliers, for example first tier and second tier suppliers, so these types of supply network systems can get quite complex.

If we look at the transportation modes that specifically serve food supply chain systems, you will sometimes have companies that use 3PLs to outsource transportation procurement but many companies still organize it internally. Truck transportation dominates most food supply chain systems, especially when you look towards the consumer end of the chains. Truck transporters are however typically involved in moving goods between manufacturers and distributors, distributors and retailers and even further up the chain as well between suppliers and production points.

Of course, there are certain food supply chain systems that require bulk transport such as rail and/or barge or inland water. When you consider import supply chain systems where there will be an international border to be crossed, you again find that the final leg of transportation is performed by truck. Such international transportation is typically an intermodal service, perhaps a sea-truck intermodal combination or an air-truck combination.

The primary reason that I wanted to show you this slide is to get you thinking about the risk in this complex system. What I've drawn here is illustrates that risk increases the further back you move along this supply chain system, where risk is a measure that captures both exposure likelihood and impact given an undetected problem. A problem that is introduced further back in the supply chain system can spread out to many distributors, retailers and then of course, consumers just by the structure of the system.

I think that the Cargill example of the corn supply chain perfectly illustrates that. On the other hand, since there are many more downstream processing steps that are potential detection points, problems that are introduced earlier in the supply chain may have a higher likelihood of detection. Clearly, there is a tradeoff here for the adversary: early introduction may lead to high impact, but also may lead to higher
Providing security to food transportation systems...

In the context of providing security to food transportation systems, it's important to understand both security vulnerabilities and concerns of freight transportation providers that serve the food industry. Other industry research groups have developed surveys to attempt to put together information to inform this point. One survey that I'd like to bring to your attention was conducted by the American Transportation Research Institute (ATRI) which is the old research arm of the American Trucking Association (ATA) which in turn is the largest trade group that serves the truckload trucking industry. ATRI put together a survey and report called, “Identifying Vulnerabilities and Security Management Practices in Agriculture and Food Commodity Transportation.”

They surveyed approximately 17,000 trucking companies that serve the food industry and received over 1,000 survey responses; responses covered a broad spectrum of the industry in terms of the size of the companies that responded as well as the types of commodities that the respondents hauled. The primary findings of this survey, released this past January, identified the primary security concerns of these transportation providers: the first one on their list was the indirect costs that carriers face to comply with various security protocols, mandates, regulations. I find that interesting.

Note that the number one concern is not how to prevent either cargo contamination or hijacking – those happen to be the next 2 – but rather is, “what are the security cost implications on my firm.” The next interesting finding from the survey addresses new security measures – the survey question, I believe asked, “What new security measures have you put into place since 9/11?” Many companies have done things new but if you look closely, note that for only one action have more than half of the responding companies done something. I think that’s also a bit interesting. This new action was to implement a driver awareness program; making drivers aware of security risks was the most common new action since 9/11.

I want to emphasize that while it’s important to identify concerns and needs, and to investigate what actions companies have taken, one missing piece in this survey is identifying the best practices. Our goal in the research that we are conducting currently with the NCFPD is to identify the effectiveness of what transportation providers are doing to provide security, along with what they should be doing based on comparison with what the best companies are doing. We would like to identify best practices, and to measure the degree of efficacy of these practices with respect to security. We’d also like to know a bit about security practices and potential efficiency gains or losses. We are conducting that study as a partner of the research team led by Dr. David Closs.

We are going to conduct our carrier survey beginning in January of 2006; we intend to cover trucking companies, both truckload and LTL, as well as railroads in the survey. We’ve done some preliminary interviews with such companies. What we’ve heard at least initially is that the truck driver is the primary concern of the trucking company, especially with regards to security but frankly with regards to everything else as well. Truck drivers are a very important component of their turnover. I think it’s also important to think about the problem of en-route security in food transportation. In a factory or facility, you usually have layers of managers, workers, quality inspectors, and security people that can oversee what is going on during food processing steps.

But while goods are en-route, a single driver is usually the only one who is in charge of that security role and I think that’s important to understand. We’ve also learned some other things. I don’t want to cover them all specifically here today, but I do want to lead into the next segment of my discussion with this final quote. Again, carriers are concerned about the indirect cost impact on their operations of security mandates or regulations. The quote that was specifically given to us is, “Will the customer that I’m providing transportation service to understand that the higher cost and the lower service that I’m now providing is due to requirements and not blame us;” a very telling perspective.

Okay; so moving to the second theme, quantifying the productivity impacts of supply chain security initiatives. I believe that it’s vital to understand the supply chain productivity implications of security processes or technology mandates. These could be either regulatory mandates that are passed down from government agencies or mandates that are imposed by customers. For example, a large food manufacturer or supplier may impose security mandates on their service providers. We need to understand and keep in mind operational productivity during this process. I think that one thing that is true is that the operational complexity of many freight transportation systems may lead to a disguising of the true cost that these companies may have to bear as a result of regulation and mandate.

Some things that may sound innocuous to someone who is not fully understanding of the complexity of running a freight system actually may have a large productivity impact. A number of researchers are trying to do economic analysis of, or cost benefit analysis of, security initiatives. The primary question is: given that I introduce security initiative A or B, where initiative A provides this level of security with this cost and initiative B provides this level of security with this cost. Often times, these cost estimates ignore productivity costs and I believe that that is a fundamental flaw because those productivity costs could be quite substantial. Then lastly, I think this is an important point; if mandates are installed that severely compromise operational productivity, you are just providing an incentive for those mandates to be ignored or not complied with. I think that is not what we want from a security point of view, so we need to understand that.

So those are the big ideas. What we are doing in terms of research – and I’m not going to have time to get into this in much detail – is that we want to develop a methodology for estimating true productivity costs of mandates for different types of mandates and different types of systems. Our fundamental assumption is that given that a mandate will be put into place, our trucking company or our transportation company is not just going to sit idly and incorporate it without many process changes. So we want to investigate how, given a mandate, would a system re-optimize itself and then given that re-optimized system, what are the productivity cost implications?

The second theme here is to search for win-win ideas where we can find security-enhancing mandates or processes or technologies that also enhance system productivity. How likely are such ideas? It’s difficult to know, and of course this likelihood varies substantially by industry. If you think about it, however, if the pure productivity cost benefit analysis did not lead to implementation of, say a track and trace system for example, it is not clear that any additional security benefit would change that analysis substantially. I think, therefore, that it will be quite difficult to find these win-win technologies, although it is certainly worthwhile to look for them. One question you need to ask here is; are certain companies just not aware of technologies that may be able to assist them from a productivity standpoint that would also help them from a security standpoint?

I don’t have time unfortunately to go through all of these examples, but I do want to say that we have looked at other regulatory initiatives and their productivity impacts in related research. For example, we’ve looked at the costs of upstream inspections – and this is in a non-food example – upstream inspections on import containers coming into the United States versus inspections at the border and what types of inventory cost implications such a regulatory mandate might impose.
on companies with high-value goods. I don’t have time to go through the details, but we compared the 2. If you look at increasing an inspection level at an upstream site, due to the fragility of the system because of sailing schedules you might see substantial growth in inventory costs, 8 to 10% growth in inventory costs where you don’t see those same growths in inventory costs if you leave the inspection system at the border the way it is currently. So again, the idea here is to try to identify hidden productivity costs of security ideas. We are also looking at a similar type of idea in the context of food trucking companies; one approach to improve security on route is to restrict operators when parking during rests, to park only in secure locations.

There are some interesting implications of this type of regulation when you look at long overnight moves and how they interact with complex US DOT hours of services regulations, and the productivity implications of this interaction. So we’ve done some initial study, and I have some preliminary slides about this topic, and not enough time to discuss them in any detail. Suffice it to say that depending on where secure locations are located on a lane, you may see significant driver requirement increases to serve the same number of loads. We’ll have more on that research topic to report on in the future. But for example, here are two different configurations of secure rest locations on a lane between Atlanta and New York; one where the total cycle time including rests is 62 h, and another with three locations where the total cycle time for drivers is 52 h. So clearly, understanding interactions between requirements and a complex operation system – even this one is very simple, it’s just 2 nodes – an origin point and a destination point – can be interesting.

Looking again on the topic of win-win security ideas, some other researchers in business schools and industrial engineering schools have looked at this issue, primarily in the area of international import containerized supply chains. There is an analogy between security and quality in such systems, and the example that I gave earlier where you try to push back the inspections to an earlier point in the supply chain, for example at an export port versus at arrival at an import port. In quality control, of course, end-of-line sampling inspections are the wrong way to do things. Instead, you want to do in-process control and prevention.

A number of the US container security initiatives attempt to implement that same idea to international transportation. One way to do that is to monitor the system via e-seals, so seals on containers that are monitored electronically as the container moves through the supply chain network. Other researchers have found that they believe that there is a win-win with such technology – so inventory cost reduction possibilities as well as security benefits for these types of systems. Some other researchers are skeptical, and claim that if there were the inventory cost benefit, the systems would already be in place. There is clearly some debate in this area. Moving finally to the last theme, the design and control of secure, cost-effective and resilient supply chain systems. In some sense, this is the big picture: resilience. Most supply chains of any type are threatened by disruptions of one sort or another, and terrorism is just one type of disruptive threat.

It is important to emphasize that recovery from disruptions is often as important as prevention. In the case of food security, that argument may not be as strong, however if you think about false positives – events that may occur that actually do not create a real security risk but are now detected by additional security processes – recovering from false positives may become an interesting operational problem.

Resilient supply chains as I define them here are ones that allow or enable cost effective recovery. I think it’s important that when we’re designing and controlling supply chain systems or transportation systems specifically, that we think about normal or nominal operations and what are the effects of initiatives and technologies on the efficiency and security of nominal operations but then also disrupted operations. Given that something has gone wrong and maybe it’s just a false positive, something that is not a real event but has caused a disruption, how are we able to recover from that event as cost efficiently as possible? From a research point of view, some of the things we are interested in are: what mechanisms in supply chains can provide resiliency? One example might be diversification of a supplier base.

If you are reliant on a single supplier and they have a problem, then you have a problem as well. It’s also important to mention that resiliency in supply chains is always possible. You can always build a resilient system, but there are clear cost implications of doing so. The interesting design question is how do we design systems that balance this cost of recovery versus nominal operating costs?

So what is the cost of providing resiliency and flexibility in our systems and then what methodologies can we use to control such systems once we’ve designed them; are there for example real time operational control technologies that enable this control? We are doing research in all of these areas. I would like to mention in closing that along with our project with the National Center for Food Protection and Defense, we also have a USDOT-funded Transportation Research Center where we are focusing on other security related problems in freight transportation. I’d be happy to share with you some of those research results if you would like to email me. In closing, the three major themes that I wanted to focus on today that it is important to both understand what companies are currently doing and where they currently believe they are vulnerable. I think it’s also important to do research to quantify productivity and practice supply chain security initiatives, primarily because of this risk of noncompliance, I think.

Also we want to make wise choices; if we are going to decide between initiative A and initiative B, and they both provide the same level of security efficacy, let’s make sure that we chose the one that also does not compromise productivity. Lastly, design and control of systems that are resilient is critical, systems such that when disruptions occur we are able to cost effectively recover.
Providing Security to Food Transportation Systems without Compromising Productivity

Alan Erera
The Logistics Institute
School of Industrial and Systems Engineering
Georgia Institute of Technology

November 4, 2005
Three major themes

I. Understand security vulnerabilities and concerns of freight transport providers

II. Quantify productivity impacts of supply chain security initiatives

III. Design and control secure, cost-effective, and resilient systems
Domestic food supply chain systems

- Supplier
- Supplier
- Supplier
- Supplier
- 3PL
- Manufacturer
- Distributor
- Retailer
- Truck transporter
- Rail transporter

Data and orders
Import food supply chain systems

Supplier → Supplier → Supplier → Supplier → Supplier → Manufacturer → Distributor → Retailer

Intermodal transporter → Truck transporter

border
Security risk tradeoffs

- Supplier
- Manufacturer
- Distributor
- Retailer

Increasing potential exposure
More potential detection points
Food transport security themes

I. Understand security vulnerabilities and concerns of freight transport providers

II. Quantify productivity impacts of supply chain security initiatives

III. Design and control secure, cost-effective, and resilient systems
Industry surveys

- “Identifying Vulnerabilities and Security Management Practices in Agricultural and Food Commodity Transportation”
  - American Transportation Research Institute, January 2005
- Surveyed 16,500+ trucking companies
- 1,023 responses
  - 50% operate fewer than 20 trucks
  - 37% 20-100 trucks
  - 13% greater than 100 trucks
- Goods hauled
  - 33% animal feed, 29% processed foods, 25% bulk beverages, ...
  - 8% live animals and fish
ATRI survey findings

- Primary security concerns
  - Indirect cost of compliance: 30%
  - Cargo contamination: 27%
  - Hijacking: 27%

- What new security measures implemented?
  - Driver awareness programs: 52%
  - Security training: 36%
  - Communications systems upgrade: 33%
  - Background checks: 32%
  - Cargo seals: 30%
  - Parking restrictions: 24%
The need for best practices

- ATRI Survey identifies *what is happening*
- Our goal: identify *effectiveness* of what is happening, and what *should happen* across industry
  - Identify best practices
  - Measure the degree to which certain practices are effective

- NCFPD Transportation Service Provider Best Practices Study
  - Carrier interviews
  - Survey January 2006
Preliminary carrier interview findings

- Driver concerns are crucial!
  - Hiring and monitoring
    - Basic criminal background checks (all)
    - More extensive screening and monitoring (some)
  - Practices to promote driver retention
    - Safety awards/bonuses
    - Driver recognition programs
  - Driver food security training
    - Some have none

- Facility security
  - Some good, some bad
  - Parking of vehicles during enroute driver rest a concern
Preliminary carrier interview findings

- Cargo sealing technology
  - Importance of customer requirements
  - E-seal adoption limited to date

- Impact of potential new federal mandates on costs and customer service
  
  “Will the customer understand that the higher costs and lower service level is due to the new requirements and not blame us?”
Food transport security themes

I. Understand security vulnerabilities and concerns of freight transport providers

II. Quantify productivity impacts of supply chain security initiatives

III. Design and control secure, cost-effective, and resilient systems
Vital to understand supply chain productivity implications of security process or technology mandates
- Regulatory mandates
- Customer-imposed mandates

Operational complexity of freight transport systems may disguise true costs

Economic analysis of mandates ignoring productivity implications may be fundamentally flawed

Mandates that severely compromise productivity likely to face non-compliance!!!
Security and productivity

1. Methodology for estimating costs of mandates
   - Assume that systems will “re-optimize”
   - Estimate optimal costs with and without mandate

2. Find security/productivity “win-win” ideas
   - Security processes or technologies that both enhance security and system productivity
   - How likely are such ideas?
     - What does the pure productivity cost-benefit analysis say?
     - Are there awareness problems?
Non-food example: potential inventory costs of upstream inspections

- CSI Port

Daily demand: $\mu = 100$, $\sigma = 20$
- If inspected containers miss sailing, booked on next
- Containers inspected with small probability $\rho$
  - Non-inspected containers on today’s sailing
  - Inspected containers: 0.8 prob today’s sailing
    0.2 prob next sailing

Carrier schedule: once every 6 days
Non-food example: potential inventory costs of upstream inspections

- No CSI

- All containers make their sailings!
- Containers inspected with probability $\rho$
  - Non-inspected containers clear Customs in 1 day
  - Inspected containers: 0.8 probability today, 0.2 tomorrow
Non-food example: potential inventory costs of upstream inspections
Productivity costs of secure parking restrictions for food transportation

- Operating cost estimation problem
  - Interaction between secure parking facility locations and driver hours-of-service regulations
  - Determine optimal driver costs:
    - When requiring rest only at secure parking facilities
    - When rest locations are not restricted

- USDOT hours-of-service regulations
  - Maximum drive time: 11 hours between rests
  - Maximum on-duty time: 14 hours between rests
  - Minimum rest time: 10 hours
Productivity costs of secure parking restrictions for food transportation

- Example single-lane problem
  - Flow Atlanta to New York metro

- Assumptions
  - Uni-directional loaded flow; all backhauls empty
  - Loads are full truckloads, with designated pickup times
  - All drivers must rest at secure facilities (terminals included)
  - Drive times deterministic

[Diagram showing the flow from Atlanta to New York with distances and secure rest locations]
Potential tours and bounds on required drivers

Configuration 1

Total cycle time: 62 hours
Minimum Drivers: maximum number of loads in any 62 hour period
Potential tours and bounds on required drivers

Configuration 2

Total cycle time: 52 hours
Minimum Drivers: maximum number of loads in any 52 hour period

Lower bound for number of required drivers smaller!
Productivity costs of secure parking restrictions for food transportation

- Current research efforts
- Driver assignment given secure parking facilities
  - Given a set of loads for a multi-week planning horizon, determine the minimum number of drivers required to serve the loads
  - Solution approach: set-partitioning integer programming model for “hard” problems
- Single-lane secure parking facility location
  - Given a repeatable set of weekly loads, determine a set of secure parking locations that will allow minimum number of drivers to perform loads
Security win-win analysis


- Quality analogy
  - End-of-line sampling inspections are wrong way to do quality assurance and security assurance
  - In-process control and prevention
- Continuous monitoring via smart e-seals
E-seal systems

- Bolt seal with RFID capability
  - Monitors presence and integrity of bolt seal, generates alarm upon bolt removal or breakage
  - Communication via RFID to readers at chokepoints
  - Minimize theft, loss and tampering

Cost
- Seals should eventually be very low (few dollars)
- Reader investment more significant
Visibility systems with e-seals

- Integration with smart seals
  - Seals can be read and status ascertained at certain “choke points”
    - Equipped ports, warehouse, factory facilities
    - Container ID, time stamps, status, seal integrity
  - Information feed to asset track-and-trace system
  - Security and integrity monitoring

- Can we document operational performance improvements?
Food transport security themes

I. Understand security vulnerabilities and concerns of freight transport providers

II. Quantify productivity impacts of supply chain security initiatives

III. Design and control secure, cost-effective, and resilient systems
Secure, cost-effective, resilient systems

- Resilience
  - Most supply chains threaten by disruptions
    - Terrorism is but one disruptive threat
  - Recovery from disruption often as important as prevention
    - Firm-level recovery
    - “False positives” important
  - Resilient supply chains allow cost-effective recovery
Secure, cost-effective, resilient systems

- Design and control of resilient systems
  - What mechanisms provide resiliency?
    - E.g. Supplier and provider diversification
  - Resiliency is always possible, but what is its cost?
  - Design and control problems
    - What methodologies allow us to design resilient systems?
      - Stochastic optimization, robust optimization, scenario aggregation approaches
    - What methodologies needed to control resilient systems?
      - Complexities introduced by coordination
      - Real-time operational control
Three major themes

I. Understand security vulnerabilities and concerns of freight transport providers

II. Quantify productivity impacts of supply chain security initiatives

III. Design and control secure, cost-effective, and resilient systems
Questions
Security win-win analysis

- Inventory model analysis of SST seal program

Lee and Whang (2003).

- $p$ = inspection probability
- $x$ = transit lead time, random variable
- $y$ = inspection dwell time, random variable
- $T$ = total lead time
Security win-win analysis

Lee and Whang (2003).

Computational study

- High-value containers ($300K), high inv cost 23%
  - \( \mu = 4300 \text{ containers/365 days} \)
  - \( R = 7 \text{ days} \)
  - \( E(x) = 30 \text{ days} \)
  - \( p' = 0.4\% \)
  - \( p = 2\% \)

- \( \sigma = \text{std dev per period demand (?)} \)
- \( k = \text{norminv}(0.95) \)
- \( \text{var}(x)^{1/2} = 6 \text{ days} \)
- \( \theta = 0.81 \) (10% reduction in std dev)

- Results: large reported savings
  - Annual inventory costs reduced from $13MM to $9MM
At the time we place order 2, we do not have the lead time for order 2. When we place order 2, we may or may not have the lead time for order 1 (and order 0, and order -1, and order –2, etc.).
Security win-win analysis questions?

- Timing of lead-time resolution from uncertain to certain is crucial
  - Advance information must arrive in time to take a valuable action
- Value of departure (CSI) inspections vs. arrival inspections

White; ongoing research (2004).

```
Supplier                                            Consignee
8                                                  0
```

```
<table>
<thead>
<tr>
<th></th>
<th>Supplier</th>
<th>Export Port</th>
<th>Import Port</th>
<th>Consignee</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>departure</td>
<td>arrival</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>0</td>
<td>T</td>
<td></td>
</tr>
</tbody>
</table>
```
Security win-win analysis questions?

Luedtke and White; ongoing research (2004).

- Assumptions
  - Order decisions made periodically, orders do not "cross"
  - Departure and arrival inspections stochastically identical
  - For departure inspections, time when containers leave origin port is known
  - Expected holding and shortage costs convex; ordering results in fixed cost per order and linear cost per item

- Dynamic programming approach
Trade growth
Global economy built on information, telecommunications, and low-cost, long-haul transport by water, rail, and air
Importance of trade to U.S. economy

U.S. Gross Domestic Product (Billions of 2002 Dollars)

- GDP Excluding Trade
- Trade in Goods and Services

GDP excluding trade and trade in goods and services from 1973 to 2002.