

# Proceedings of The Institute of Food Technologists' First Annual Food Protection & Defense Research Conference

November 3-4, 2005  
Atlanta, Georgia

[Session: Transportation and the Supply Chain]

## Dimensioning a Secure Supply Chain

DR. DAVID CLOSS  
MICHIGAN STATE UNIV.

**T**hank you very much Alan. It's indeed a pleasure to be here. Based on some of the questions that we've been hearing this morning I think the common theme that's coming out is how do we implement some of these security practices?

I want to discuss a research project that we're involved with, again, under the sponsorship of the National Center for Food Protection and Defense. It's a joint project between the Michigan State Univ., the Univ. of Minnesota and Georgia Tech. It's a trans-disciplinary project as well integrating perspectives of supply chain, quality, and security.

The goal of that project is to create a tool for use by both large firms such as Cargill as Mr. Sims mentioned but also by smaller firms to identify supply chain practices that make a difference when enhancing security. So the question is: What are the key processes and how can a firm assess and improve what its doing to enhance supply chain security?

As proposed to the National Center, this project focuses on the flow of food products from the commodity supplier through manufacture through some type of logistics and distribution system to the retailer and ultimately to consumers. In addition to focusing on production processes, this includes the need to manage and enhance the security at other stages in the supply chain particularly in transportation vehicles and warehouses, distribution centers as well as at the retail store. In this research, we are trying to focus on the supply chain elements that are often forgotten because they aren't highly visibility. This project evolved from work that Ed McGarrell, the Director of MSU's School of Criminal Justice, and I did under the sponsorship of IBM in 2004.

IBM requested a white paper that could characterize supply chain security from both supply chain and security perspectives. The security perspective focuses on what do to keep people out of the facility and to keep product in the facility. The supply chain focuses on what to do to move product efficiently and effectively as Mr. Sims discussed. The white paper synthesized the lists of activities to enhance supply chain security provided by firms and institutions. The lists are prioritized in terms of basic security activities, typical security activities, and advanced security activities for each activity level, the white paper identified specific activity dimensions in terms of relationships with customers, suppliers, carriers and employees. While we believed that the white paper made a contribution, the question that kept coming up was whether the activity levels could be quantified further. About the same time the Broad Agency Announcement for the National Center was released and we decided to focus the quantitative assessment on the food industry.

The triangle of, from the Criminal Justice literature, illustrates that terrorism requires simultaneous convergence of three elements. It requires an offender or the terrorists. The terrorists must have access to the product on the lower left or what is called the target. On the lower right is a location, a location that not secure. From a criminal justice point of view, the triangle is a relatively representative situation. When viewed from a supply chain perspective, it is a little more complex because the product flows through the supply chain quickly. It is necessary to protect the product throughout the supply chain not just at one particular point.

So the focus of the research is to identify what are the processes that a firm, a supply chain and even an industry have to organize to dissect this triangle, to take one leg out of it and keep terrorists away from the product or keep terrorists away from the location where they could damage the product.

Although the Supply Chain and Information Technology research team study includes 5 projects, this discussion will focus on the first 3; those involving MSU, the Univ. of Minnesota, and Georgia Tech. The final 2 projects are being directed by Keith Helferich who will focus on them. The first project begins with a benchmarking assessment regarding what companies are doing.

The assessment first identifies company activities and then creates a tool that facilitates benchmarking their practices against those of other firms in the food industry and other divisions within their own firm. The benchmarking and assessment project focuses on the entire supply chain including commodity providers, manufacturers of food products, wholesalers, institutional wholesalers, retailers and transportation providers.

This project began with focused discussions with representatives from each member of the food supply chain regarding their practices and their effectiveness. The goal is to create a spreadsheet tool that would be made available to any firm which can be used to benchmark their food supply chain security performance. The result of the research will be an understanding regarding the dimensions of security practices being used by firms and the relative effectiveness in terms of performance. The 4th and 5th projects conducted under the leadership of Dr. Helferich focus on specific supply chain security standards and supply chain incident management.

The goal of the overall Supply Chain and Information Technology research is to develop a data base and information tool to guide best practice sharing for improving supply chain security efficiency and effectiveness. Similar projects have been completed on three other

occasions by the supply chain faculty at Michigan State. The previous work has focused on overall supply chain performance competencies rather than the rather limited area of security.

This project is focusing specifically on food supply chain security. The objective is to create a spreadsheet tool that would be able to characterize what firms do by commodity, by size of firm, and by location within the channel. As indicated previously, this part of the project involves MSU, Univ. of Minnesota, and Georgia Tech. Each institution is focusing on a different element of the distribution channel with MSU focusing on manufacturers and wholesalers, Minnesota focusing on food service providers and retailers, and Georgia Tech on logistics service providers. In each case however, we are asking similar questions regarding what can and should a firm do to enhance food supply chain security?

The IBM white paper developed a very extensive list regarding the guidelines for firms to enhance food supply chain security. This research is attempting to refine that, structure it, organize it, and consider what should a firm do in terms of its suppliers and customers? Other considerations are: (1) What should a firm do in terms of its internal processes with employees and facilities? (2) Where does a firm stand with respect to the various stages of security management?, and (3) What relationships does the firm have with suppliers, with carriers, with the government that can enhance food supply chain security performance? While the white paper had categorized performance in terms of basic, typical and advanced, this research is designed to use Likert-scaled behavioral scores regarding how well the respondent believes his or her organization has considered or implemented security practices. The result is a series of competencies—the terms I am using today to describe practices, philosophies, capabilities—that characterize the broad grouping of activities that firms are using to enhance food supply chain security.

This research is designed to identify the competencies that a firm requires to enhance the overall supply chain security and what is the relative impact of each competency. The literature review and discussions with supply chain participants identified ten competencies. The MSU interviews focused on manufacturers, wholesalers, and commodity suppliers. The Minnesota interviews focused on retailers and food service wholesalers while Georgia Tech focused on carriers and service providers.

Next, survey was developed to obtain quantitative responses regarding firm supply chain security practices. While the surveys for the various supply chain institutions are similar, each has some unique questions to adapt to specific channel institutional issues. The survey is going to be released during the first quarter of 2006. At this point, the survey has been piloted, reviewed, refined in terms of terminology, how firms think of security, how firm would respond, and testing various forms of communication. The testing has been a fairly extensive process to insure research quality.

Simultaneously, the team has developed the diagnostic spreadsheet framework to facilitate both data collection and to facilitate benchmarking by individual firms. Some firms have requested the option to benchmark themselves across divisions. In this case, the five plants representing the divisions each respond to the survey and compare their performance across the various dimensions of security. The goal of the divisional benchmarking is to be able to allow the firm to determine if corporate and the divisions are all on the same page in terms of security, its importance, and terminology. It will allow a large firm to benchmark across divisions to see how the different divisions perceive their security capabilities.

Then by using it across industries and channel stages, it will allow a firm to benchmark them selves against other stages or commodity types. The research will also allow firms to benchmark by firm size to reflect the fact that large firms may demonstrate differ levels of

performance from smaller firms. Our next step is to survey the industry, analyze the data, and incorporate the specific benchmarks for the high performing firms. Our previous research has defined the high performing benchmark as one standard deviation above the mean.

When targeting and speaking with firms, this research is taking a cross functional approach or trans-disciplinary approach. A very interesting aspect of this research is the interchange between supply chain, criminal justices, and food safety. By bringing these disciplines together, the research team has learned the characteristics, the names, the terminology and the concerns of the other disciplines. Based on the literature, the research team has identified a framework incorporating ten competencies that characterize supply chain security performance. The competencies are necessary to provide food supply chain security with both efficiency and effectiveness.

Within this framework, the ten security competencies need to be created, orchestrated, and managed within and across each firm in the supply chain. These competencies have been conceptualized by synthesizing the current literature and extensive interviews with over 50 supply chain, security, and food quality managers representing over 20 firms. These include: (1) process strategy; (2) process management; (3) infrastructure management; (4) communication management; (5) technology management; (6) process technology; (7) metrics; and (8) relationship management; (9) service provider collaboration management; and (10) public interface management. In the present context, security competencies are defined as the synthesis of selected security capabilities into a logically coherent and manageable state of affairs sufficient to gain and maintain supply chain security. Competencies have been used often to describe best-practice frameworks in logistics research.

An important note about the framework is that each of these competencies applies to every member of the supply chain. Figure 3 implies that manufacturers, retailers, and logistics service providers are no different in their need for, and application of, each of the competencies. Each competency occurs within each supply chain partner at both the “overall” (for example, corporate) and local (for example, warehouse, manufacturing site) level. In addition, relationship management, communication management, and shared metrics need to exist between supply chain partners to improve the overall level of security. Figure 3 implies that metrics serve a dual purpose. First, each firm in the supply chain has its own metrics by which it measures its security capabilities. This firm centric use of metrics cuts across 5 other competencies: process management, infrastructure management, communications management, management technology, and process technology. Therefore, firm centric metrics measure the effectiveness of firm security capabilities over each of these competencies. Second, each firm has the responsibility of communicating these metrics to other firms in the supply chain. These ovals represent the competencies that tie each supply chain partner together in their communication of security related information. Effective use of relationship management, service provider management, and metrics are needed not just between one partner to another, but across the entire supply chain to increase the effectiveness of terrorist threat planning, speed of detection, appropriateness of response, and efficiency of recovery.

Process Strategy is executive commitment to security and fostering a security culture is a necessary condition for implementing an effective security environment. Top management needs to encourage frank discussions regarding the importance of security, both for the safety of stakeholders and in maintaining the value of the firm's brand. Top management must be visible in their commitment and dedication to implementing security initiatives. As an example, some firms have created a “chief security officer” position among the top management team to provide additional structure to security initiatives. Additionally, through training and sharing of threat information, executives foster a culture among personnel that places security among their top priorities.

Process management describes the initiatives taken to ensure the security of each activity involved with the acquisition, receipt, manufacturing, and storage, and movement of materials into and out of a facility. Process management includes the use of simulated incidents to test the integrity of procedures and processes. A key element of process management is the formalization of processes, for material receipt, shipment, and handling. It also includes the formalized disaster management process and evaluates the degree to which the firm has put planning, detection, response, and recovery procedures into place. Simulated incidents may include table-top exercises designed to test the effectiveness of a firm's security capabilities.

As the name implies, process management also involves the in-depth knowledge, and management, of firm processes. This is necessary to identify vulnerabilities that may be exploited by malfasants. Additionally, firms who increase their process knowledge may discover redundant, or unneeded, activities. Discontinuing these activities could reduce firm overhead and process variability leading to lower costs and improved service levels. This is one avenue through which firms may find synergies in security that allow for operational improvement as well as an increase in security competency.

Infrastructure management refers to the manner in which a firm secures its physical premises and products. This includes employee/non-employee access control for facilities (or areas within facilities), employee background checks, securing empty and loaded trailers before/during transport, and guards, among other measures. These are the most basic, and commonly thought of, steps to increase security and serve to form a "perimeter" that guards against unauthorized entry into a given space. Firms need to develop strategies for controlled sharing of potential threat and security information internally with employees and providing communication channels for employees to use when a potential threat exists or an incident occurs. Firms need to develop threat awareness and security training programs. Similarly, the working environment may need to be changed to acknowledge unknown personnel in a facility. In this sense, communication management is related to process strategy. Communication management tools are used to implement a security culture.

Communication management may also simultaneously increase security and operational performance. This will occur if security related communication requirements increase interdepartmental contact and break down "silos". For example, if the purchasing and manufacturing functions have not previously communicated regarding security until they begin sharing security related information, it is possible that they could begin sharing non-security related information (for example, ways to schedule receipts of purchased materials to match the production schedule), which could improve firm performance.

Management technology refers to the ability to detect potential security threats or incidents, and share timely and reliable information internally and externally. Information systems provide a first defense mechanism by which to understand trends in product contamination, missing shipments, and the root causes of these occurrences. These information systems also play a critical role in gathering information that is subsequently shared with suppliers, customers, 3rd party service providers, and government agencies to identify potential problems or recovery actions at the intersection between firms.

Process technology involves the presence, use, and ability of information systems to track the movement of products and monitor processes internally and across the supply chain. Process technologies include the use of tracking technologies, such as Radio Frequency Identification (RFID) and smart-seals, and process improvements.

Most firms have not progressed beyond implementation of physical security measures (for example, gates, guards, and cameras) and have not garnered the advantages that may come from tracking technologies. Previous work has found that equipping containers with smart-seals, electronic seals that track the movement of supply chain assets through global positioning systems (GPS) and/or RFID, effectively reduced administrative overhead, improved labor productivity, lowered transaction costs, reduced theft, and induced savings in safety stock and overall supply chain inventory (Buxbaum 2003). Process technology is one avenue to explore to derive synergistic benefits from security.

Security metrics involves the continuous development, use, testing and redefinition of guidelines measuring security related procedures, plans, and capabilities. Metrics might be implemented to comply with specific guidelines, such as those of a customer or government agency, or the firm may develop specific guidelines for which metrics are captured and evaluated. Similarly, a firm may conduct audits or have an external entity certify that current procedures and processes are in place to increase security.

The previous competencies are critical to the discussion of supply chain security as any supply chain protection program is only as strong as its weakest link. Collaboration with external entities (customers/suppliers and separately, service providers) is necessary to ensure that security procedures are communicated and followed (Sheffi 2001). Global relationships present added security difficulties as the focal firms are unable to monitor their partner and protect against theft, contamination, or insertion of unauthorized counterfeit cargo.

These competencies may represent another means by which firms may uncover operational synergies through increasing security. Communicating security related information with supply chain partners and service providers may help firms to form closer bonds with these entities and encourage collaboration on other, non-security related issues (for example, sharing demand figures or promotional information).

Public interface management describes the security related relationships and exchanges of information with the government and the public. Forging relationships with U.S. government agencies is a critical corporate capability to more fully protect the firm against terrorist acts. Firms may actively guide and participate in the development of government standards or security initiatives. Similarly, firms should develop well-defined processes for systematically monitoring and synthesizing information coming from public entities regarding possible threats while at the same time developing processes to communicate with appropriate government officials and the public should an incident occur.

The purpose of this work was to present a supply chain security framework to guide practitioners and researchers in their future initiatives. Practitioners have been uncertain where they should begin to secure their supply chains. This uncertainty reflects a preponderance of existing recommendations with few explicit standards. This work brings together practitioner and academically oriented literature from different disciplines and details a comprehensive framework to guide managers in this respect.

Little academic work has been devoted to supply chain security. This framework is designed to serve as a roadmap for future investigations. Supply chain security holds promise for interested researchers. Primarily, research is needed in the area of security best practices. Little is known regarding what security actions industry leaders have taken and how this compares to other firms who are not as advanced.

# Dimensioning a Secure Supply Chain

Dr. David Closs

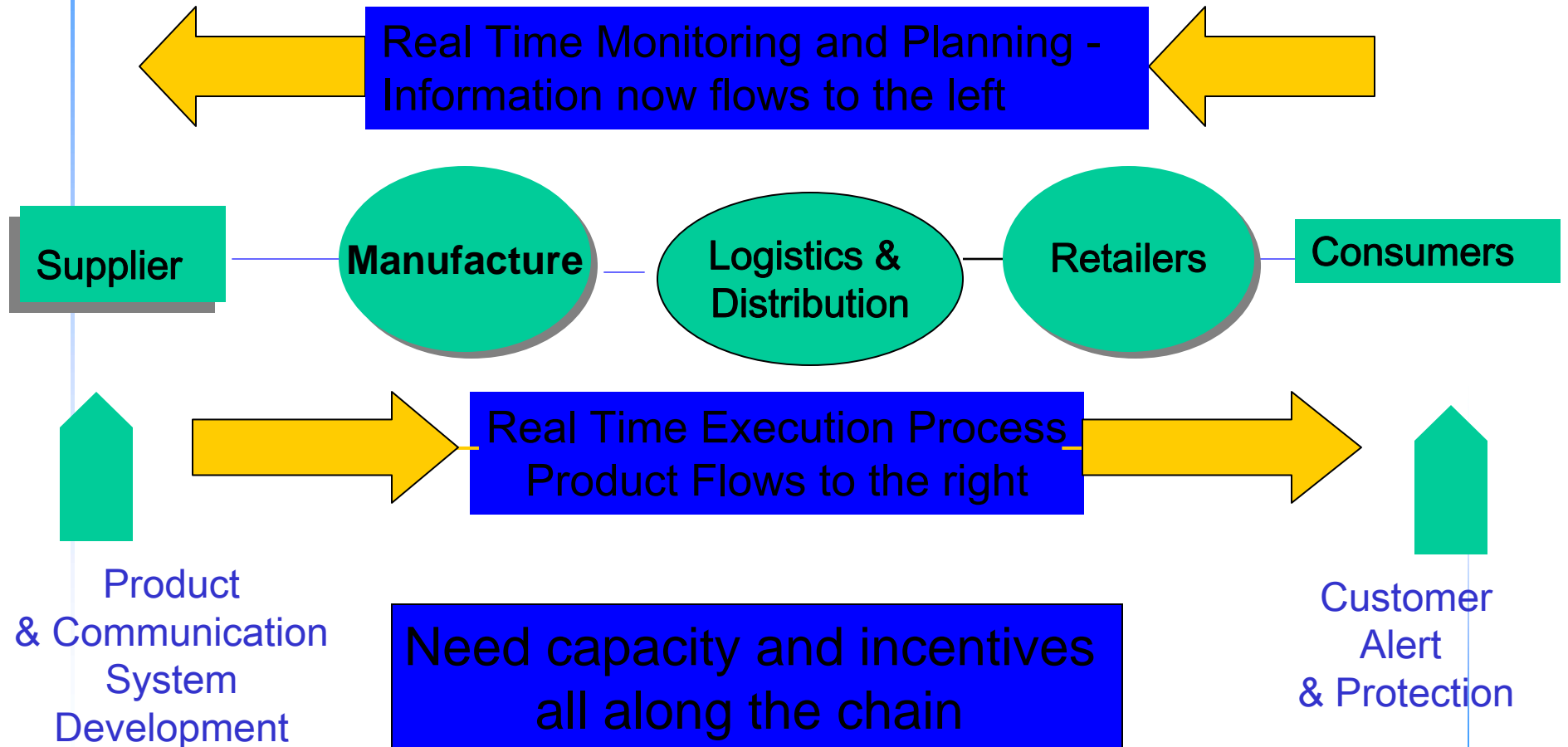
John H. McConnell Chaired Professor

Michigan State University



**THE LOGISTICS INSTITUTE**  
Georgia Institute of Technology  
[www.tli.gatech.edu](http://www.tli.gatech.edu)

# Supply Chain Network– The Scope

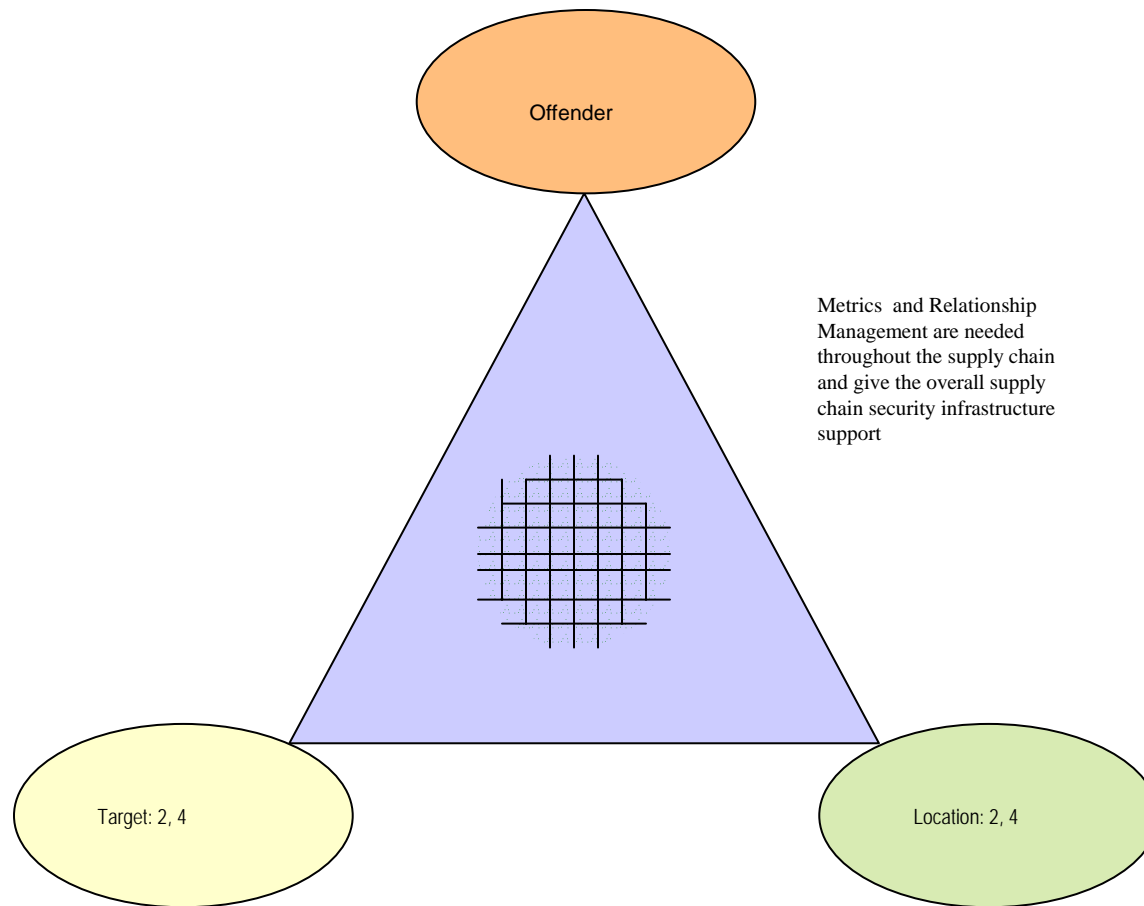


# Definition of Supply Chain Protection and Security

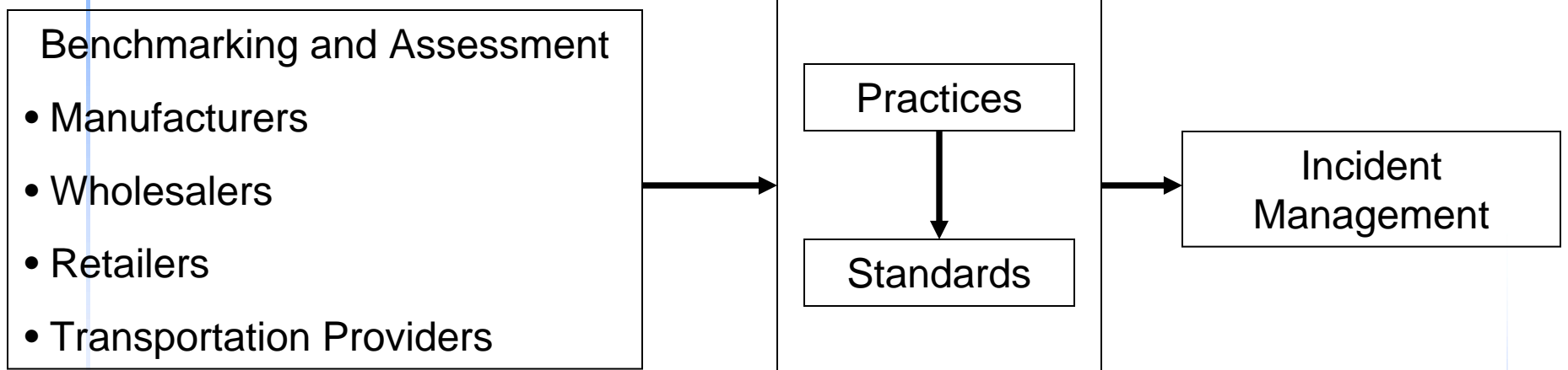
- The application of policies, procedures, and technology to protect SC assets (product, facilities, equipment, information, and personnel) from theft, damage, or terrorism and to prevent the introduction of unauthorized contraband, people, or weapons of mass destruction.
  - ✓ Closs and McGarrell (2004)



# The Triangle of Crime



# Study Components




# Benchmarking and Assessment

- Goal
  - ✓ Developing data base and information tool to guide best practices for improving efficiency and effectiveness sharing throughout the food chain
- Projects
  - ✓ Summary and assessment of supply chain best practices
  - ✓ Development of new supply chain best practices recommendations



# Benchmarking and Assessment Lead Researchers



UNIVERSITY  
OF MINNESOTA

Dr. Jean Kinsey

Applied Economics

Wholesalers, Retailers, & Restaurants



MICHIGAN STATE  
UNIVERSITY

Dr. David Closs

Supply Chain Management

Suppliers, Manufacturers, & Distributors



Dr. Alan Erera

Transportation and Logistics

Transportation Providers

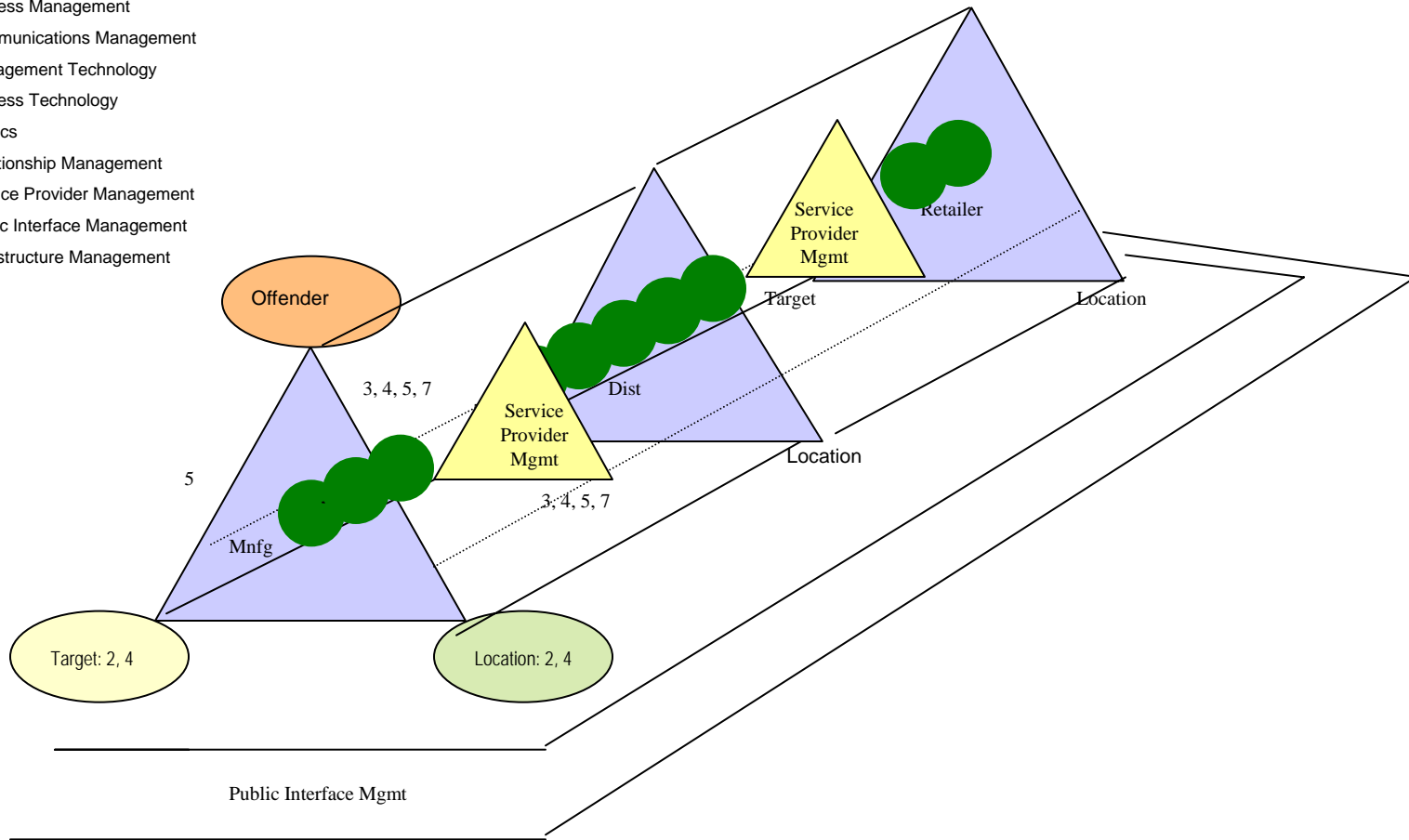
# Practice Assessment

- What can and should firms do?
  - ✓ Relationships with suppliers and customers
  - ✓ Internal processes - use of electronic – real time communications
  - ✓ Incident and security management stages
- What can and should those that provide major system support functions do?
  - ✓ Government
  - ✓ Carriers
  - ✓ Terminal/Port operators
- Practice rating
  - ✓ Basic/Typical/Advanced
  - ✓ Likert scaled behavioral scores
  - ✓ Security performance characteristics (Incidents, cost, asset utilization, resiliency)



# Food Supply Chain Security Competencies

1. Process Strategy
2. Process Management
3. Communications Management
4. Management Technology
5. Process Technology
6. Metrics
7. Relationship Management
8. Service Provider Management
9. Public Interface Management
10. Infrastructure Management



# Research Design

- Company interviews
- Survey development
- Survey piloting, review, and refinement
- Spreadsheet development
- Survey industry
- Analyze data
- Incorporate benchmarks into spreadsheet
- Document

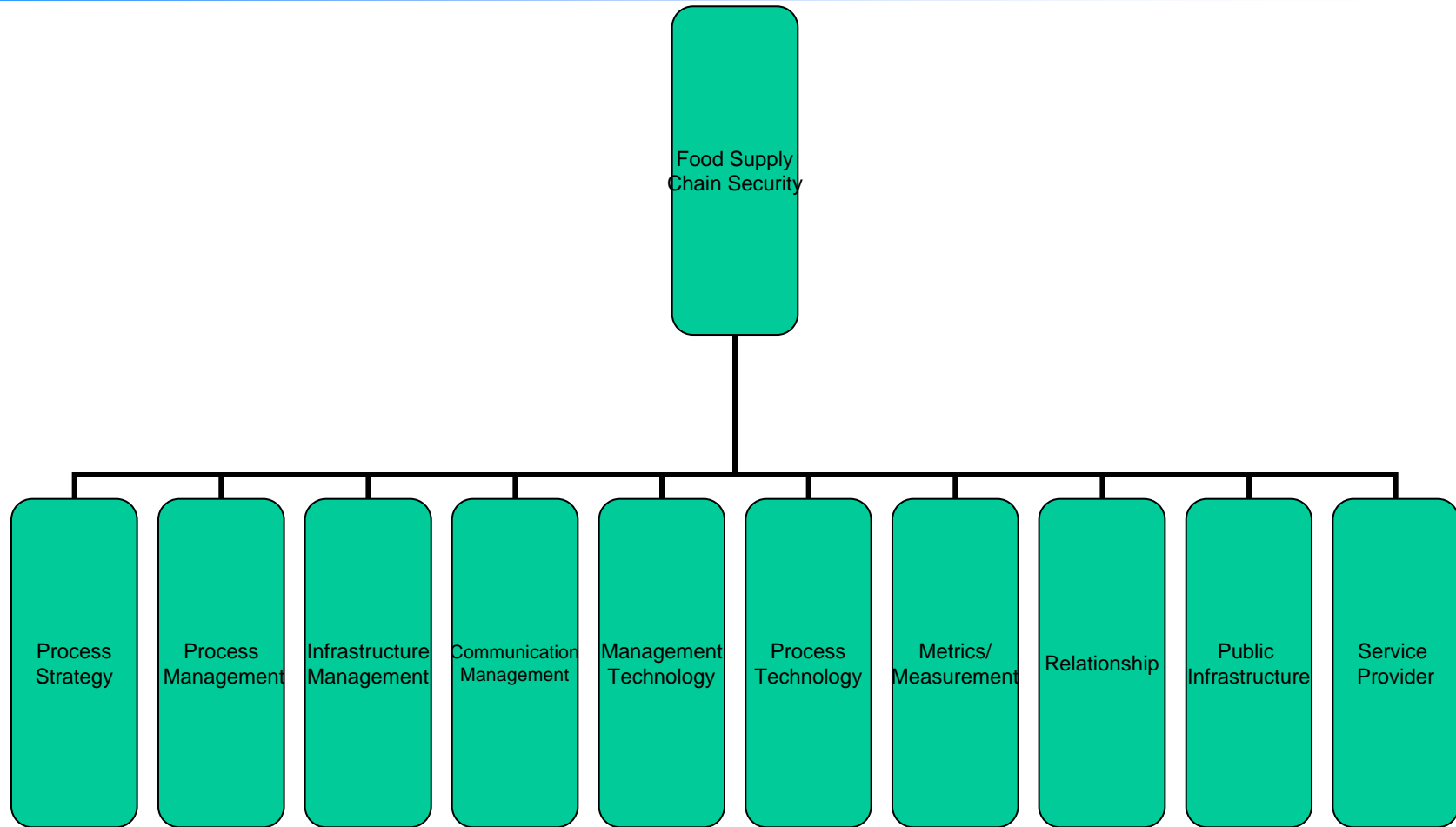


# Interview Model

- Contact company and provide project description
- Obtain agreement for participation
- Send functional questionnaire
  - ✓ Quality
  - ✓ Supply chain
  - ✓ Security
- Arrange for on-site interviews with general questions



# Competency Performance drives Security Performance



# Survey Samples

- Manufacturers/Wholesalers
  - ✓ Manufacturers Association
  - ✓ Institute of Supply Management (Food industry)
  - ✓ American Society of Industrial Security
- Retailers
  - ✓ Top 200 retail food companies
  - ✓ Top 200 food service companies
  - ✓ Top 100 retail food wholesalers and food service distributors
- Transportation
  - ✓ American Trucking Association



# Competency Definition

- Process Strategy – Enterprise philosophy regarding the importance of food supply chain security.
- Process Management – How people do things, procedures for dealing with internal operations (shipping, receiving, handling, etc.)
- Infrastructure Management – Presence of gates, guards, fences, seals on containers/trailers/rail cars. Security checks on employees.
- Communication Management – Training, education, and internal communications.



## Competency Definition (Continued)

- Management Technology – Information technology at the collaboration and company level. Designed to facilitate collaboration and information sharing regarding security breaches.
- Process Technology – Diagnostics, tracking systems to monitor processes.
- Metrics/Measurement – Guidelines regarding how security is measured
- Relationship Management – Relationships with suppliers and customers.



## Competency Definition (Continued)

- Public Interface Management – Relationships with government and public.
- Service Provider Management – Relationship with carriers, warehouses, and other service providers.



# Process Strategy Characteristics

- Firm's senior management believes security provide competitive advantage.
- Firm's senior management believes security is necessary to protect brand.
- Has a senior management position focusing on security.
- Firm believes security initiatives are a cost of doing business.



## Process Management Characteristics

- Employs guidelines from FSIS.
- Uses test incidents to test supply chain protection capabilities.
- Employs HACCP throughout the supply chain.



# Infrastructure Management Characteristics

- Maintain empty trailers in secure environment.
- Access control to critical enterprise infrastructure.
- Maintain restrictive controls.
- Maintain loaded controls in secure environment.
- Access control for employees.



# Communication Management Characteristics

- Incorporates recovery information in food security awareness training.
- Defined communication protocols for internal use.
- Incorporates response information in food security awareness.
- Defined communication protocols with NIMS.
- Incorporates prevention information in food security awareness.



## Management Technology Characteristics

- Provide valid information to supply chain partners regarding security incident responses.
- Provide timely information to supply chain partners regarding security incident responses.
- Provide valid information to supply chain partners regarding security incidents.
- Provide timely information to supply chain partners regarding security incidents.



# Process Technology Characteristics

- Uses RFID technology to track products when outside firms control.
- Ability to track and trace products up and down one level.
- Uses GPS to track containers.
- Has technology to track products including salvaged, reworked, and returned product.



# Metrics/Measurement Characteristics

- Implemented company security metrics based on industry guidelines.
- Implemented supply chain security metrics based on company guidelines.
- Implemented company security metrics based on company guidelines.
- Implemented supply chain security metrics based on government guidelines.



## Relationship Management Characteristics

- Uses historical information from security audits to determine if relationships should be maintained with customers.
- Applies specific education programs for supply chain partners regarding security procedures.
- Defined consequences for supply chain partners who fail to comply with security procedures.
- Uses supply chain security audits for frequently used suppliers.



## Public Interface Management Characteristics

- Understands the public's expectations during crisis incident response.
- Participates in emergency-preparedness planning with appropriate government agencies.
- Participates in emergency-preparedness tests.
- Collaborates with public health groups.
- Established a risk/disaster communications strategy for media/public.



## Service Provider Management Characteristics

- Collaborates with service providers to improve security programs.
- Verifies service provider qualifications.
- Verifies that service providers monitor origination of service supplier assets.
- Requires service providers to implement controls that prevent food product contamination.



# Performance Metrics

- Detection
- Reduced incidents
- Resilience
- Risk profile
- Reduced costs
- Improved productivity
- Improved customer service
- Meet security expectations



# DIAGNOSTIC RESULTS

## COMPETENCY RESULTS

Supply Chain Security Benchmarks		World	
	Firm	Class	Gap
Scale: Strongly Disagree 1 2 3 4 5 Strongly Agree	Mean	Benchmark	
Process Management	#DIV/0!	0.00	#DIV/0!
Process Strategy	#DIV/0!	0.00	#DIV/0!
Infrastructure Management	#DIV/0!	0.00	#DIV/0!
Communication Management	#DIV/0!	0.00	#DIV/0!
Management Technology	#DIV/0!	0.00	#DIV/0!
Process Technology	#DIV/0!	0.00	#DIV/0!
Service Provider Management	#DIV/0!	0.00	#DIV/0!
Metrics/Measurement	#DIV/0!	0.00	#DIV/0!
Relationship Management	#DIV/0!	0.00	#DIV/0!
Public Interface Management	#DIV/0!	0.00	#DIV/0!
<b>Overall Score</b>	<b>#DIV/0!</b>	<b>0.00</b>	#DIV/0!



# Benchmark Process

- Benchmark within the division
  - ✓ Sensitivity by site
  - ✓ Consistency by site
  - ✓ Activities
- Benchmark across the firm
  - ✓ Sensitivity by site
  - ✓ Consistency across divisions
  - ✓ Activities
- Benchmark across industry
  - ✓ Industry performance



## **“Quality and Security are the same things now. Everybody has to have both.”**

- Increased focus on Internal Access Control and Monitoring
  - ✓ Building a “challenge” culture
  
- Increased focus on intentional contaminations
  - ✓ Procedures, Training, Discipline
  - ✓ Disgruntled employees (and ex-emps) and external threats
    - Several companies activities were informed by disgruntled employee incident



## Security is Strategic

- **Executive level cross-functional security councils**
  - ✓ Strategic Planning, Communications and Operations
  - ✓ Every company reportedly has an active council/committee
  - ✓ Industry and company (executive through employee) awareness has increased
  
- **Brand Protection is essential to business**
  - ✓ Security is value-added, not marketing tool
    - One competitor reportedly promoted shopping cart handle wipes
  - ✓ “Want to be confident, but not a target”



# Technology Increases Security

- Every company has Track and Trace capabilities
  - ✓ Levels of specificity to source and monitoring nodes vary significantly
    - Several companies report “total recall” abilities
- CCTV is almost universal in corporate and distribution facilities
  - ✓ Farm side facilities more difficult to secure
- Seals are (almost) universally used
- RFID and GPS are not universal or real-time
  - ✓ Performance and cost/benefit issues



**“Quality used to be an internal concern; security was external. Now, they’re integrated.”**  
**Improved Process (and some lowered costs!)**

- ✓ Supply/Aggregation
  - Increased distribution capacity reduced (3<sup>rd</sup> party) costs
- ✓ Transportation
  - Enhanced scheduling and control reduced load/off-load times (and overtime)
- ✓ Security (Monitoring)
  - Cameras captured accident; allowed retraining, reduction of insurance premiums

▪ **Cost/Benefit Assessment**

- ✓ Too early to tell for most companies
- ✓ Improved customer service in terms of timing and product pedigree



# Questions and Discussion



**THE LOGISTICS INSTITUTE**  
Georgia Institute of Technology  
[www.tli.gatech.edu](http://www.tli.gatech.edu)