DIGITALCOMMONS
— @WAYNESTATE —

Journal of Transportation Management

Volume 23 | Issue 1

Article 3

4-1-2012

Understanding supply chain security strategy

Zachary Williams
Central Michigan University, zac.williams@cmich.edu

Jason E. Lueg
Mississippi State University, jlueg@cobilan.msstate.edu

Sean P. Goffnett
Central Michigan University, sean.goffnett@cmich.edu

Stephen A. LeMay
University Of West Florida, slemay@uwf.edu

Robert L. Cook
Central Michigan University, Robert.cook@cmich.edu

Recommended Citation

Williams, Zachary, Lueg, Jason E., Goffnett, Sean P., LeMay, Stephen A., & Cook, Robert L. (2012). Understanding supply chain security strategy. Journal of Transportation Management, 23(1), 7-25. doi: 10.22237/jotm/1333238520

UNDERSTANDING SUPPLY CHAIN SECURITY STRATEGY

Zachary Williams
Central Michigan University

Jason E. Lueg
Mississippi State University

Sean P. Goffnett
Central Michigan University

Stephen A. LeMay
University of West Florida

Robert L. Cook
Central Michigan University

ABSTRACT

In the post-9/11 environment, organizations are acutely aware of the need to secure their supply chains from risks of being a target of, or an unwilling participant in, a terror attack. However, supply chain security (SCS) comes at a cost and increasing levels of protection have increasing levels of costs to the firm. So some firms engage in strategic initiatives to secure the supply chain (SC) while others do not; and each firm engages in varying degrees of activities to ensure SCS. Therefore, in this study, the researchers sought to explore what types of SCS strategies exist. The researchers analyze 162 responses to a SCS survey completed by executives from a broad range of firms and industries and identify three general SCS strategies: Advanced, Laggards, and Compliant. Implications for researchers and practitioners are presented.

INTRODUCTION

The events of September 11, 2001 were a catalyst for change in many supply chain operations. Supply chain security issues and initiatives have affected numerous firms (Yang and Wei, 2013). At a minimum, firms want to protect their property and investments. From a larger perspective, firms want to protect society. Clearly, no firm wants its name permanently linked to the next 9/11-like attack. However, Supply Chain Security (SCS) can be difficult to understand and ultimately implement. SCS is unique because if it is working well, it remains virtually invisible. As a result, little is known about SCS strategies.

Understanding strategy is at the core of supply chain research (Christopher et al. 2006; Tokman et al. 2007) and it is through firm strategy formulation that cost/benefit considerations are weighed (Tang, 2006). But supply chains, particularly those that are multimodal, are vastly complex (Scholliers et al. 2012), where a multitude of firms in any given network will employ a myriad of strategies. As a result, academicians have dedicated efforts to understanding them, and in some cases guiding them. Research on supply chain strategies has examined the relationship between corporate strategy and SCM (Hofman 2010); logistics strategies (Autry et al. 2008) and logistics activities in relation to firm performance (Lynch et al. 2000); postponement versus speculation (Pagh and Cooper 1998); and changes to strategy based on environmental factors (Atwater et al. 2010).

Most research on SCS strategies falls into the latter category: changes to strategy based on environmental factors. The stream of research on SCS strategies is growing. Empirical work has led to a greater understanding of SCS strategies in the food industry (Whipple et al. 2009) and in transportation (Voss et al. 2009b). Empirical research has also uncovered antecedents to implementing SCS practices (Williams et al. 2009a), SCS as an organizational culture (Williams et al. 2009b), and the development of a SCS orientation (Autry and Bobbitt 2008), among others.

Williams et al. (2008) reviewed the literature on SCS and highlighted several issues related to this research. First, there are few empirical studies on SCS, but SCS practices and strategies may be difficult to capture because firms avoid discussing SCS. This may be because firms want to conceal their practices to keep them secure, but it may also be because they want to conceal that they have no real strategy and no real practices.

Second, research on SCS has a narrow scope and focuses on few industries, often only one industry. The industries most often studied are those most likely to engage in SCS, so it may not present a holistic view of SCS. For example, Whipple et al. (2009) focus on the food supply chain. This excellent study, while insightful, gives results only for the food industry and the findings may not apply elsewhere. In addition, Martens et al. (2011) use food firms as a control variable in their research, which might indicate that food firms have lower levels of perceived security performance than do other firms. However, most firms and most industries have likely been affected by SCS, whether they welcome the effects or not; the number of security practices and government programs are evidence of this. Thus, a broader cross section of industries will give a better perspective on SCS, what firms are doing, and how SCS affects outcomes.

Third, SCS practices are often prescribed based on norms that lack a research foundation. For example, Helferich and Cook (2002) suggest firms approach SCS the way the Federal Emergency Management Agency (FEMA) approaches disaster management. FEMA prepares for disruptions through planning, mitigation, detection, response, and recovery; a layered approach that goes beyond deterrence and prevention. Sarathy (2006) and Sheffi (2005b) support a different kind of layered approach, one where each layer of security enclosed still another, so if the first is breached, a second or third still remains to protect the chain. This normative work is an important step in developing a research foundation on SCS. It establishes a point from which empirical work can begin and offers important starting points for practitioners who are trying to figure out what to do next in a climate that has changed radically after 9/11.

Given the gaps in previous research, along with recent calls for more strategic supply chain research (Fawcett, Waller, and Bowersox 2011), the current study has the following objectives: first to analyze primary survey data from respondents representing a broad range of firms and industries and second; to determine what SCS strategies, if any, exist among the broad range of firms. The following sections review literature on SCS and SC strategy and present the methods and analysis used in the study before discussing the results and implications for researchers and practitioners.

LITERATURE REVIEW

This literature review highlights the key points in SCS research that are tied to the objectives of this study. It is not intended to be a comprehensive review of SCS literature. For a comprehensive review of the SCS literature, readers are referred to Williams et al. (2008).

SCS Research

SC management requires security because of the complexity, dependence, and extended trust and commitment between SC partners (Sarathy

2006); and although individual firms have created SCS measures within the firm, these measures fail to address the rest of the SC (Sheffi 2005a). Unfortunately, to date, the logistics and SCM literature have been slow to provide help in understanding SCS and best practices (Closs and McGarrell 2004; Hale and Moberg 2005). In summarizing existing SCS literature, Rice and Spayd (2005) suggest that three themes emerge: little empirical evidence, many examples of reaction to past events, and no investigations into current corporate responses.

SCS Strategy

It would be hard to argue that SCS should be initiated as an organizational strategy (Trunick 2005), but SCS strategies remain remarkably clear. The normative work from the earliest part of the century is partly responsible for this. When Helferich and Cook (2002), described the need for SCS strategy in terms of FEMA's approach to disasters, they laid out a clear path for those in need of immediate help and security. This and other early work on the subject (e.g., Sheffi 2005a) foreshadowed some strong empirical work.

Martens et al. (2011) surveyed 62 executive-level supply chain personnel and found that proactive security approaches, internal and external security planning, vulnerability of nodes, and measuring security performance are all significant influencers of security effectiveness. Their finding also indicates that the control variable of "firm type" leads to effectiveness outcomes and that firms involved in the food industry find lower levels of perceived security effectiveness than do firms in other industries.

Also, in a comprehensive analysis of 199 respondents (which remains as one of the largest data sets in SCS research), Voss et al. (2009b) evaluated the strategic security nature of the firm, internal and external approaches to SCS, and perceived security performance; and found two clusters—high and low performing supply chains—that related to security performance. They found when firms place more importance on security they also perceive more security implementation and better security performance.

Voss et al (2009a) examined 130 responses in a conjoint analysis concerning supplier selection and SCS. Their responses came from purchasing managers, members of the Institute of Supply Management (ISM) and the American Purchasing Society (APS). They found differences in buyer preferences for security versus price and delivery reliability along two characteristics: 1) domestic versus international sourcing; and 2) concern or lack of concern over previous incidents experienced by the firm. For domestic sources, buyers chose price over security, although the results were mixed—importance scores supported this result, but market simulations did not. In the simulations, buyers who were concerned about prior incidents did trade price for higher levels of security. For domestic sources, buyers unequivocally chose high reliability over advanced security, even if they were concerned about prior incidents.

For international sources, buyers were more likely to choose advanced security over price and even to choose advanced security over delivery reliability. Voss et al. (2009a) suggest that the price/reliability dichotomy for choosing suppliers remains strong and that security does not overwhelm either. Firms seeking the lowest price may move away from security if it adds to costs. Firms seeking high delivery reliability may choose in favor of advanced security, but only if it does not compromise delivery reliability in domestic trade. In international trade, buyers may compromise delivery reliability for advanced security. The authors noted that these results may not apply in other industries (Voss et al. 2009a).

Williams et al. (2008) expanded on the dichotomous, internal-external approach to strategy. They found four major categories of strategic focus in SCS: firms that stress intraorganizational activities (internal), firms that stress inter-organizational activities (external), firms that stress both (combination), and firms that ignore SCS altogether.

Elements of SCS Strategy

Security techniques and tactics range from purchasing mandated requirements for supplier security, to locks and RFID tags, to security audits, and participation in government programs like C-TPAT (e.g., Voss et al. 2009b). The following represent some of the most important security practices discussed in the literature.

SCS Culture

Arguably, SCS culture may be the most important and most heavily researched area in the field (e.g., Rice and Spayd 2005, Quinn, 2003, Christopher and Peck, 2004; Sheffi, 2005b; Williams et al. 2009b). Previous research has shown the need for creating a SCS culture (Sheffi 2002; Sheffi 2005b) and for rewarding such buy-in (Whipple et al. 2009). Failure to reward buy-in to the SCS culture can allow security programs to become stale (Quinn, 2003) or to be abandoned. Williams et al. (2009b) suggest a culture of security is critical to SCS. Practitioners have responded similarly. For example, Schneider International, a leading transportation and 3PL provider, boasts of building a culture of security in their overall effort to secure the SC (Ritchey 2010). In the current study, SCS culture is defined as the overall organizational philosophy that embraces and projects norms and values that protect the SC and engage employees in protecting the SC (Williams et al. 2009b).

Security Communication

SCS depends on the efforts of many firms throughout the SC (Closs and McGarrell 2004), so firms must communicate to share vital information. As a result, to build security, firms must develop communication strategies to share that information (Closs et al. 2008). When supply chains have communication plans in place and share security related information, increased security cooperation and reduced risks are likely to result (Manuj and Mentzer, 2008). The sharing of critical information can be used proactively (to prevent a security breach) or reactively (to minimize a breach or assist in response).

Examples of communication and information sharing include: setting security expectations and sharing these expectations among SC partners; developing a common security communication infrastructure (e.g., EDI requirements, GPS, RFID technology); sharing real-time SCS monitoring/detection status information (e.g., Homeland Security Advisory System); providing feedback from security audits; providing communications that direct SC efforts in a coordinated response to a security threat; and sharing communications that enable SC partners to begin recovery from a disaster (Helferich and Cook 2002).

Organizations that are working together in the physical flow of goods rely on one another for sharing and disseminating information. Security requirements have increased information sharing and communication expectations. Security communication is defined as the ability for all SC members to grant, share, and transmit critical information to one another to ensure that the SC will be protected.

Operational Modification

Goods now flow through the supply chain in a different way because firms have adopted SCS strategies. These changes, labeled operational modifications, have been necessary to secure the supply chain. A wide range of activities have been modified for security. Examples of operational modification include reducing or increasing the amount of inventory held at a given stocking location. For instance, some firms are increasing all inventory levels as a safety precaution while others are only increasing "critical supplies." Other firms have decentralized inventory by adding inventory stocking locations to reduce risk. Sheffi (2002) proposed the notion of a dual inventory system.

In this system, a small amount of inventory designated as strategic emergency stock is held and only used in extreme situations to keep operations running. These modifications to inventory policies have a resulting impact on transportation decisions as well.

Other firms have made drastic changes to manufacturing operations. Williams (2008) suggests that some firms are moving to JIT manufacturing models to reduce inventory levels. The reduced levels of inventory provide less opportunity for security breaches. However, Martha and Subbakrishna (2002) suggest that JIT operations results in extra risk because a disruption may lead to a production shutdown and, as a result, customer dissatisfaction and defection. Also, some firms are developing redundant production capabilities for critical products or contingency production capability (Helferich and Cook 2007). Regardless, the notion is the same: firms are making changes so they can feel more secure.

Transportation operations have seen security changes as well. Some firms have made decisions to change modes to improve shipment security. Rather than reduce cost and introduce potential security breaches, some shippers have switched to speedier, safer modes, such as air, for their shipments. Recent pirate attacks on ocean shipments and the resulting insurance increases have accelerated this practice. Williams (2008) also provides examples of shipments of caravans (deploying a group of trucks out at once) and increased usage of truckload shipments (fewer touch points) as other operational changes to transportation. Overall, operational modification is defined as changes to core SC activities, including operational procedures, manufacturing, inventory levels, and/or transportation in an effort to create SCS.

Access Restriction

Access restriction is an SCS activity that involves limiting where, when, and how people can enter SC facilities, use SC equipment, or touch materials, equipment and facilities (Min, 2012). This is in congruence with other research and initiatives (e.g., ISO 28001: 2007) that mentions tactics such as: controlled access points, employee verification, special doors and gates, card readers, visitor procedures, finger ID, gate passes, and limiting access for both internal and external personnel. This activity can be described as knowing who has access to what at all times, thus resulting in increased security. Access restriction can be considered critical because it provides a better understanding of who is entering SC facilities, where they can go once inside, what is being brought into SC facilities, and what information and materials are getting out. Specifically, this may include restricting the access of visitors, vendors, truck drivers, and even in some cases, a firm's own employees. By allowing unknown people only in known areas, firms are reducing the possibility of any unauthorized personnel introducing contraband into the supply chain. Therefore, access restriction helps secure an organization by letting everyone know who and what enters their physical locations.

Security Services

Increasingly, firms have become interested in outsourcing security activities. These outsourcing security initiatives are a key to the way that firms create SCS. Most firms lack expertise in security, so they seek partners who have the expertise. The rationale is much the same as for outsourcing other logistics or SC activities. Security firms have the expertise in one or more areas of security; firms in most other industries do not have people with this level of expertise.

Many firms outsource security services for special situations (escorting high-value shipments) or for guarding facilities and transportation full-time. Steinman (2004) found that half of 103 senior executives in his survey of transportation firms would hire firms that specialize in physical security services. Williams (2008) found that these security firms might provide armed secure transport, helicopter escort of truck shipments, off-duty police and ex-military personnel at facilities, employee or candidate background check services, and installation of monitoring equipment. Partnering with these firms helps to create a secure supply chain. External security services are defined as the outsourced protection of the SC to firms or people who specialize in such protection.

Security Inspection

The process of inspection can be viewed as assuring that everything is in the proper order and operating condition to permit the secure operation of the SC. Examples of inspections include: physical inspection of goods, tampering inspections, and tiered inspections. These inspections are conducted by using human efforts and technology, such as metal detectors. This process is intended primarily to prevent SC disruptions.

Inspection is a broad security effort. For manufacturers and retailers, inspection could be evaluation of inventory and inspection of deliveries. For manufacturers, inspection could be the evaluation of production activities to ensure no contraband has been introduced into those operations. For transportation providers, inspection may be verifying the physical contents and quantity of shipments and assuring that no contraband is being moved. SCS Inspection is defined as checking products, operations, and processes to prevent security breaches.

METHODOLOGY

Following is a discussion of the measurement variables and the sample collection.

Measures

In this study, a survey instrument used new construct measures for the independent variables of security communication, operational modification, access restriction, security services, and security inspection. Another independent variable used in the study, Supply Chain Security Culture (SCSC), was a previously developed scale (Williams et al. 2009b). In addition, demographic (respondent's job title, annual sales revenue for the firm, in what industry the organization operates, and the firm's position in the SC) and firmographic (SCS breaches, SCS responsibility, and SCS focus) data were collected about each respondent's firm. The firmographic data was collected in order to better understand any possible security strategies.

There were several dependent variables captured in the survey. The purpose of capturing these variables was to understand and explain differences in SCS security strategies. As a result, three dependent explanatory variables were captured. For the variable *security breach*, respondents were asked to indicate the degree to which their firm had suffered a serious supply chain breach (1=Strongly Disagree; 7=Strongly Agree). This single item was then split into high security breach (responses of 6 or 7), medium security breach (3, 4, or 5) or low security breach (1 or 2). For *SCS responsibility* respondents were asked to self classify their firms' attitude on responsibility of SCS by indicating if SCS was their own (internal) responsibility or the responsibility of all supply chain partners, including governments (external). This internal/ external dichotomy is consistent with prior research (c.f., Williams et al. 2008; Voss et al., 2009b; Martens et al. 2011). Finally, for *SCS focus* respondents were asked to classify their firms' attitude as either being primarily focused on preventing SCS breaches or on responding to security breaches once they occurred. This dichotomy is similar to prior suggestions on prevention versus response as general security approaches (c.f., Mitroff and Alpaslan 2003; Arntezen 2010).

The items for each of the measures (except for demographics and firmographics) are found in Appendix A. All scaled items used a 7-point Likert-type response scale (1=Strongly Disagree; 7=Strongly Agree). Although it is beyond the scope of the study presented here, all these measures were grounded in initial qualitative research and subjected to the steps presented in

Churchill (1979). This includes a review of all the measures by panels of academic experts and practitioner experts. The survey was refined based on the expert panel comments and then pretested through a survey of supply chain and logistics professionals who were alumni of a university based in the Midwestern United States. The pretest produced 65 responses, a 30% response rate and allowed the researchers to establish the performance of items and constructs before launching the main data collection.

Sample Collection and Characteristics

The sample was obtained from the Council of Supply Chain Management Professionals (CSCMP). Due to the sensitive nature of the topic (security) it was suspected that there would be a low response rate since people in charge of security are not inclined to talk about it or to respond to surveys about it. Therefore, a goal was to solicit many respondents in order to obtain as many usable responses as possible. Also, given the strategic-level nature of the research topic, respondents in executive and managerial roles with relatively large amounts of responsibility and knowledge of the questions being asked were targeted. Responses from titles such as CEO, VP, Director, and Manager were sought. The sample purchased from CSCMP included 2,996 individuals who met these criteria. When, organizational redundancies were eliminated (i.e., cleansing the contact database so that only one respondent per firm was asked to complete the survey), a sample of 1,753 firms remained. In total, 62 usable responses (a 3.5% response rate) were obtained from the CSCMP sample. This response rate, while low, is similar to other research using the CSCMP database (e.g., Lewis 2006).

This small number of responses prompted the researchers to get another sample from a marketing research firm. The same criteria as with the CSCMP database was used: one response per firm from an executive working in an applicable industry (manufacturing, carriers, 3PLs, warehousers/distributors, and retailers). This original sample included 3,500 firms. After eliminating overlap with the first sample and firms in non-targeted industries (i.e. consultants), the final sample size was 2,774. From the adjusted sample, there were 100 usable responses (a 3.6% response rate).

Two tests had to be run with the data before analysis. First, the main question with the separate samples was whether or not the data should be combined as one group. An ANOVA was conducted for the items across the samples and the results indicated no significant differences existed between the two samples. Thus, the data sets were combined into a final dataset of 162 useable responses, representing 162 unique firms, with no redundancies. The number of useable responses from respondents at this level (C-level), from exclusive firms, concerning this topic, compares favorably to other research on this topic (e.g., Voss et al. 2009a, b; Martens et al. 2011). Next, the database was then divided into two groups (early and late) based on the electronic time stamps that were recorded upon submission. Differences between early and late respondents were evaluated using ANOVA. The ANOVA results suggest that non-response bias was not an issue with this study. Finally, although missing data was not an issue with this study, a handful of missing values were replaced using mean values.

The overall sample characteristics are found in Table 1. The job title of the respondent is most often a Director (25.3%), VP (24.1%), or Manager (21.6%). Of the named categories, respondents are most often found in Consumer Packaged Goods (24.2%), Electronics (9.3%), or Medical/Pharmaceuticals (6.8%). But it should be noted that the largest industry category is Other (36.0%). Relative to SC company role, the largest group of respondents identify themselves as manufacturers (45.7%) and the second largest as 3PLs (19.1%). Annual sales in dollars are most often greater than one billion (36.9%).

TABLE 1
OVERALL SAMPLE CHARACTERISTICS*

Variable	n	%
Job Title		
President/CEO	19	11.7%
C-Level	13	8.0%
EVP/SVP	12	7.4%
VP	39	24.1%
Director	41	25.3%
Manager	35	21.6%
Industry		
Automotive	6	3.7%
Medical/Pharmaceutical	11	6.8%
Apparel/Textiles	7	4.3%
Electronics	15	9.3%
Industrial Products	8	5.0%
Consumer Packaged Goods	39	24.2%
Chemical/Plastics	9	5.6%
Appliances	3	1.9%
Agriculture	5	3.1%
Other	58	36.0%
SC Position		
Manufacturer	74	45.7%
Carrier	11	6.8%
Wholesaler/Distributor	15	9.3%
Freight Forwarder	4	2.5%
3PL	32	19.1%
Warehouser	8	5.6%
Retailer	11	6.8%
Other	7	4.3%
Annual Sales		
$1-$1M	2	1.3%
$2M-$25M	28	17.5%
$26M-$100M	29	18.1%
$101M-$1B	42	26.3%
Greater than $1B	59	36.9%

* N=162

RESULTS AND FINDINGS

Psychometric Properties

To assess unidimensionality, a factor analysis using PCA and Varimax Rotation (Netemeyer, Bearden, and Sharma 2003) was conducted. Once construct unidimensionality was confirmed, scale reliability using Cronbach's alpha in SPSS was examined. The resulting alpha values range from .837 to .960 (see Appendix A), which exceed Nunnally and Bernstein's (1994) recommended guideline of .70. After unidimensionality and reliability of each construct was confirmed, PCA with Varimax Rotation was used to assess validity of the constructs. As Appendix A shows, all items loaded on the constructs as expected. Furthermore, all items correspond to one and only one factor, with most factor loadings well above .70. This offered evidence of validity. The assessment of the psychometric properties suggested sound measurement so the next step was to explore security strategies.

Cluster Analysis

Since the primary purpose of this study was to determine whether SCS strategies exist, a three-step cluster analysis process was used to evaluate security strategies. Cluster analysis is often used in strategic SC and logistics research (e.g., Autry et al. 2008; Whipple et al. 2009). Cluster analysis groups respondents on similarity, while maximizing the dissimilarity between clusters (Hair et al. 2006). If the sample is heterogeneous (i.e., clusters exist), then the clusters will be described using attitudinal and firmographic variables, which is consistent with prior research using this technique (e.g., Williams et al. 2011)

The cluster analysis was conducted on the six key security variables (SCS culture, security communication, operation modification, access restriction, security services, and security inspection) that emerged from the literature review. A multiple step clustering process follows the suggestion of previous research (i.e., Reynolds and Beatty 1999). This was done because no statistical techniques can determine the appropriate number of clusters, so the process remains to some extent subjective.

In the first step, it is suggested that the appropriate number of clusters should be approximately between n/60 and n/30, where n is the size of the sample (Lehmann 1979). Using the n/60 to n/30 rule of thumb, three to six clusters is deemed to be appropriate for this analysis (162/60 and 162/30).

In the second step, hierarchical cluster analysis was used to identify the number of clusters, based on Ward's method, with a squared Euclidian distance measure. This method is recognized for its ability to maximize homogeneity within clusters, while at the same time maximizing heterogeneity between clusters (Aldenderfer and Blashfield 1984) and is recommended because it results in clusters with the smallest sum of squares error (Arabie and Huber 1994). The largest percentage change in the agglomeration schedule was evaluated for clusters between three and six (which were determined in the first step). According to this result, the largest change in the agglomeration schedule comes when three clusters are merged into two. This indicates that a three cluster solution may be most appropriate for this sample.

Finally, the last step was to identify clusters using a non-hierarchical technique (K-means). Non-hierarchical techniques do not use a step-wise function like hierarchical techniques. Instead, this procedure assigns cases to clusters once the optimal number of clusters (seeds) has been identified (Hair et al. 2006). Cases are classified by moving the cases into groups when they are close to the mean vector of a group (Landau and Everitt 2004). The numbers of clusters determined during the hierarchical stage were used as seed points for the K-means process. The K-means cluster analysis yielded three clusters of 31, 71, and 60 respondents in each.

The case membership of the clusters was saved in SPSS as a new variable. This allowed for further analysis in determining an appropriate number of clusters. According to Hair et al. (2006), all clusters should be significantly different on all clustering variables. With three clusters established, a test was conducted to determine if the clusters differed on all the clustering variables. A one-way ANOVA was used with the three clusters as independent variables and all SCS activities as the dependent variables. At the .001 level of significance, the ANOVA results indicated that there were significant differences among the clusters on the clustering variables. This finding indicates that a three cluster solution represents unique SCS strategies. Results from the ANOVA are presented in Table 2.

TABLE 2
ANOVA RESULTS FOR CLUSTER DEVELOPMENT

Security Variables	P-Value	Cluster 1 Means	Cluster 2 Means	Cluster 3 Means
SCSC	0.000	2.88	5.77	4.29
Op Mod	0.000	4.67	6.15	5.87
AR	0.000	4.62	6.57	6.18
SS	0.000	2.23	4.69	2.87
Inspect	0.000	3.42	6.31	5.56
Comm	0.000	3.30	5.84	5.07

With clusters developed, and different security strategies revealed; demographic variables, along with attitudinal variables, were analyzed to describe each cluster.

Cluster Interpretation

For discussion purposes, each cluster was named. The cluster name was developed from the "theme" of the cluster as assessed through the variable means. Naming clusters based on themes of the groupings follows best practice in supply chain and logistics research (e.g., Williams et al. 2011). Based on the results, the clusters were labeled as: 1) The "Laggards"; 2) The "Advanced"; and 3) The "Compliant". Table 3 shows demographic descriptions of each cluster. Additional descriptions of the clusters follows.

Cluster 1: The "Laggards"

These firms represent 19.1% of the sample and are comprised primarily of manufacturers (61.3%); are in the consumer package goods (CPG) industry (12.9%); and have sales of $26M-$100M (33.3%). The slight majority view SCS as an internal responsibility (55.2%); have a response focus (58.6%); and overwhelmingly do not feel that they have experienced a serious SCS breach (80.0%). In terms of security perceptions, this cluster had the lowest scores on all six SCS strategy elements, in comparison to other segments. As a result, this group is named the "Laggards" for discussion purposes.

Cluster 2: The "Advanced"

This cluster represents the largest portion of the sample at 43.8%. This cluster is mostly comprised of manufacturers (33.8%) and 3PLs (25.4%); are involved with CPG industry (28.2%); and have annual sales in excess of $1B (39.4%). The vast majority view SCS as the shared responsibility of all supply chain partners (78.9%); have a prevention focus (93.0%); and is the cluster with the greatest perception that their firms have experienced a serious SC breach (8.5% have a high perception and 25.4% have a medium perception). In terms of security perceptions, this cluster had the highest scores on all six SCS strategy elements, in comparison to other segments.

Cluster 3: The "Compliant"

This cluster is the second largest part of the sample with 37.0%. In this cluster, 51.7% identified themselves as manufacturers; as with the previous two clusters, the majority are in the CPG industry (25.4%). In terms of sales, 40.7% have sales of greater than $1B. The majority view SCS as the shared responsibility of all supply chain partners (71.7%); have a prevention focus (75.0%); and is the cluster with the lowest percentage of serious supply chain breach (1.7%). Firms in this cluster scored in the middle on all attitudinal scores related to SCS, in comparison to other segments.

DISCUSSION OF RESULTS

The first goal of this research was to understand if more than one approach to SCS exists. The cluster analysis reported here supports this finding; the categories that emerged from the analysis follow a proactive (Advanced), do the minimum necessary (Compliant), or try to do as little as possible (Laggard) approach. An interesting finding is that there is good representation across the three clusters relative to annual sales, industry, and SC position. That is, the three strategies identified are not exclusive to any particular industry, SC position, or firm size; rather, each strategy is found in practice regardless of demographics. This supports the generalizability of these findings. Also, within cluster rankings of activities do not vary much between the three groups (i.e., Advanced and Compliant both rank Access Restriction as number one; Laggards and Compliant rank Inspection as number three; all three clusters rank Communication, SCS Culture, and Security Services as number four, five, and six, respectively). However, the groups vary significantly on the intensity in which they do each activity.

Laggards have likely given little thought to engaging in holistic security activities and may

TABLE 3
CLUSTER DEMOGRAPHIC PROFILES*

Variable	Cluster		
Annual Sales	**Laggards (N = 31; 19%)**	**Advanced (N= 71; 44%)**	**Compliant (N = 60; 37%)**
$1-1M	0.0%	0.0%	3.4%
$2M-25M	16.7%	22.5%	11.9%
$26M-100M	33.3%	14.1%	15.3%
$101M-1B	26.7%	23.9%	28.8%
$1B+	23.3%	39.4%	40.7%
Industry			
Automotive	3.2%	4.2%	3.4%
Medical/Pharmaceutical	6.5%	4.2%	10.2%
Apparel/Textiles	0.0%	7.0%	3.4%
Electronics	9.7%	9.9%	8.5%
Industrial Products	6.5%	5.6%	3.4%
CPG	12.9%	28.2%	25.4%
Chemical/Plastics	6.5%	7.0%	3.4%
Appliances	3.2%	2.8%	0.0%
Agriculture	3.2%	2.8%	3.4%
Other	48.4%	28.2%	39.0%
SC Position			
Manufacturer	61.3%	33.8%	51.7%
Carrier	9.7%	7.0%	5.0%
Wholesaler/Distributor	3.2%	11.3%	10.0%
Freight Forwarder	0.0%	5.6%	0.0%
3PL	16.1%	25.4%	15.0%
Warehouser	3.2%	7.0%	3.3%
Retailer	3.2%	7.0%	8.3%
Other	3.2%	2.8%	6.7%
SCS Responsibility			
Responsibility is Ours	44.8%	21.1%	28.3%
Responsibility of All	55.2%	78.9%	71.7%
SCS Focus			
Prevention Focus	41.4%	93.0%	75.0%
Response Focus	58.6%	7.0%	25.0%
Security Breach			
High Perceived SC Breach	3.3%	8.5%	1.7%
Med Perceived SC Breach	16.7%	25.4%	25.0%
Low Perceived SC Breach	80.0%	66.2%	73.3%

view SCS as a necessary evil. These firms had the lowest scores for each SCS strategy element. It is likely that this group views SCS as a forced requirement as opposed to a strategic activity. This is supported by the fact that, of the SCS strategy elements, Operational Modification is ranked highest by Laggards. These modifications might be required of the Laggards by their supply chain partners. It may even be that these firms attempt to avoid SCS altogether. This segment did indicate a low perceived security breach to their supply chain, which may contribute to this stance on SCS strategy. Some firms simply do not or cannot justify SCS costs and gamble that a SC breach is a low risk for them. Further, if SC partners are implementing SCS, some partner firms may not feel an obligation to spend resources on security. For instance, many U.S. ports have not taken an aggressive approach to SCS initiatives (Thibault et al. 2006); thus, many shipping organizations have indicated taking little security efforts (Rice and Spayd 2005). Furthermore, Laggards might not be as involved with complex SCs and thus view SCS as their own issue and are less expectant of others assuming responsibility for SCS. It also may be why these firms are primarily focused on responding to rather than preventing security breaches.

The firms that fall into the Compliant group have different tendencies in regard to SCS. Compliant tend to comply with accepted security practice. They have most likely seen the Advanced-cluster firms develop some SCS practices and then have attempted to emulate some of those best practices – just not to the degree to which the proactive firms have. These firms may also be suppliers to Advanced firms, making it necessary for them to comply with proactive practices imposed by their customers. Interestingly, this cluster has the lowest perception that they have experienced a serious supply chain breach. This adds support to the perception that these firms might be "forced" to be compliant by external partners. In addition, these firms are more prevention focused than Laggards but not to the degree that Advanced are. The firms within this group are about 'average' or 'middle of the road' in their approach to SCS. They are not the proactive firms like the Advanced group, but they are doing more than the bare minimum for SCS.

Advanced approach security proactively. This group is dedicated to a holistic SCS approach as they scored highest in all security activities. It is likely that this group of firms is capable of dedicating many resources to enhancing SCS with Access Restriction and Inspections ranked as the most important. This is most likely because these firms experience the highest perception that a high security breech has already occurred in their SCs. Thus these firms are heavily prevention focused and view SCS as the responsibility of all SC members – not just their own. Perhaps this perception of shared responsibility for SCS causes these firms to collaborate more with supply chain partners and, therefore, they are both required to and, in turn, require others to integrate many SCS elements into their strategies.

CONTRIBUTIONS, LIMITATIONS, AND FUTURE RESEARCH

This section addresses the academic and managerial contributions of the research, some research limitations, and suggestions for future research.

Contributions to Literature

Although this is an exploratory study, it does make contributions to the body of knowledge by advancing the understanding of SCS and related strategies. First, this research describes SCS strategies that organizations implement to create security in the SC. It has been suggested that firms need to approach SCS from a strategic perspective (Sarathy 2006). Unfortunately, academic research has not provided specific strategic options for firms to adopt in order to secure their supply chain. This research is one of the first to identify and describe detailed activities and overall SCS categories and is consistent with prior strategy research in developing a strategy taxonomy (e.g., Galbraith and Schendel 1983; Hawes and Crittenden 1984; Lassar and Kerr 1996; Autry et al. 2008; Ashenbaum and Terpend. 2010; Keller et al. 2010).

Contributions to Practice

Managers can benefit through identification of the strategies discovered in this research. Managers can identify what category their organizations fall into and then assess their strength within that strategy cluster. This research identifies three main ways that firms can approach securing the supply chain. These approaches were named: Advanced, Compliant, and Laggards. As mentioned earlier, no firm wants its reputation associated with a catastrophic event, especially if the post-event investigation might find that they could have done something to prevent it, but chose not to do so. No organization wants the label "Laggard" after the fact.

Limitations and Future Research

The sensitive nature of this study most likely resulted in the low response rate; however, a higher response rate might have yielded different findings so this response rate should be noted as a limitation of the current study. Furthermore, other SCS strategy activities could provide alternative results. Future studies might investigate other types of SCS strategy elements, such as government programs (C-TPAT).

In this sample, the Advanced and Compliant clusters had the majority of their firms classified as having annual sales in excess of $1B while the Laggard majority was $26M-100M. Are Laggard firms Laggards because they have fewer firm resources to deploy towards SCS or are they simply too small to require such advanced practices? Are Advanced firms larger because they have more advanced SCS practices or are they simply able to spend more on SCS because they are larger? Future research needs to address a causal relationship of security practices on performance to answer "does security cause performance"? In addition, the use of the firmographic variables of SCS responsibility and SCS focus presented interesting results here and should be evaluated further. Also, future research may validate the security strategies presented here in another sample. Finally, additional research should empirically address the drivers of supply chain security strategies. In other words, what forces predict membership in a particular security strategy cluster?

RESEARCH CONCLUSIONS

As supply chains become increasingly global, firms must adopt strategies for the secure flow of goods from raw material to end consumer. Furthermore, as security issues are increasing in importance to many end consumers, this will likely force all SC members to take a new look at security measures to ensure consumer satisfaction; but these measures will come at a cost to both firms and consumers. The findings of this study will assist organizations as they develop strategies for the implementation of SCS practices.

APPENDIX A
SCALES/ITEMS, SCALE RELIABILITY, AND FACTOR ANALYSIS

Scale/Item (Scale Alpha)	Item Mean	Std. Dev.	Item-to-Total	λ
Operation Modification (α = .951)				
Thinking about our supply chain strategy, our company makes changes to…				
…the way our supply chain operates.	5.72	1.192	.882	.875
…specific supply chain activities.	5.81	1.076	.941	.904
…how our supply chain operates with suppliers.	5.76	1.074	.879	.893
Access Restriction (α = .837)				
Thinking about our supply chain strategy, our company…				
…creates restricted access areas at our facilities.	6.05	1.341	.673	.713
…creates designated areas where visitors are allowed within our facilities.	6.13	1.211	.748	.802
…strictly controls all access to our facilities.	5.98	1.266	.681	.827
Security Services (α = .849)				
In regard to our supply chain strategy, our company…				
…chooses to work with specialized security firms to create supply chain security.	3.93	1.794	.831	.845
…creates security in the supply chain by working with external security firms.	4.06	1.849	.808	.844
…chooses to place the responsibility of supply chain security on external security firms.	2.65	1.434	.556	.805
Inspection (α = .934)				
Thinking about our supply chain strategy, our company…				
…checks for any contraband in our product/services to prevent them from being distributed.	5.58	1.675	.835	.812
…takes efforts to check for potential security breaches before our product/service is delivered.	5.42	1.583	.868	.798
…diligently looks at products and processes before being delivered to prevent security breaches.	5.43	1.619	.888	.807

APPENDIX A
SCALES/ITEMS, SCALE RELIABILITY, AND FACTOR ANALYSIS
(Continued)

Communication (α = .951)				
In regard to our supply chain strategy, our company makes sure…				
…our supply chain members keep us informed of new supply chain security developments. (Adapted from Morgan and Hunt 1994)	5.19	1.424	.851	.740
…our supply chain members communicate their supply chain security expectations clearly. (Adapted from Knemeyer et al. 2003)	4.91	1.455	.869	.782
…our supply chain members let each other know as soon as possible of any unexpected problems with supply chain security. (Adapted from Anderson and Narus 1990)	5.13	1.45	.877	.809
…our supply chain members agree to share critical information among all chain members to ensure supply chain security.	4.99	1.46	.822	.827
…to communicate with other supply chain members to ensure supply chain security.	5.12	1.469	.906	.821
SCS Culture (From Williams et al. 2009b) (α = .960)				
Thinking about our supply chain strategy, our company…				
…creates a supply chain security focus among all employees.	5.01	1.69	.852	.854
…makes sure that supply chain security is the first thing on the mind of all employees.	4.11	1.77	.857	.855
…makes supply chain security the norm for all employees.	4.68	1.70	.923	.908
…dedicates efforts to create a supply chain security-focused workforce.	4.70	1.78	.906	.871
…makes sure that all employees are vigilant toward supply chain security.	4.84	1.70	.906	.889

REFERENCES

Anderson, J. C. and Narus, J. A. (1990), “A Model of Distributor Firm and Manufacturer Firm Working Partnerships,” *Journal of Marketing*, 54(1): 42-56.

Arntezen, B. 2010. “Global Supply Chain Risk Management Part 1: Differences in Attitudes, MIT CTL White Paper, available at http://ctl.mit.edu/library global_supply_chain_risk_ management_pt_3_differences_practices;

Ashenbaum, B. and Terpend, R. (2010), “The Purchasing-Logistics Interface: A “Scope of Responsibility” Taxonomy,” *Journal of Business Logistics*, 31(2): 177-194

Autry, C. W. and Bobbitt, M. (2008), “Supply Chain Security Orientation: Conceptual Development and a Proposed Framework,” *International Journal of Logistics Management,* 19(1): 42-64.

Autry, C. W., Zacharia, Z. G. and Lamb, C. W. (2008), “A Logistics Strategy Taxonomy,” *Journal of Business Logistics*, 29(2): 27-52.

Aldenderfer, M.S. and Blashfield, R. K. (1984), *Cluster Analysis*, London: Sage Publications.

Arabie, P. and Huber, L. (1994), Cluster Analysis in Marketing Research, in: Bagozzi, R.P. (Ed.), *Advanced Methods in Marketing Research*. Oxford: Blackwell, 160–189.

Atwater, C., Gopalan, R., Lancioni, R., and Hunt, J. (2010), "To Change or Not to Change: How Motor Carriers Responded Following 9/11," *Journal of Business Logistics*, 31(2): 129-156.

Christopher, M. and Peck, H. (2004), "Building the Resilient Supply Chain," *International Journal of Logistics Management*, 15(2): 1-14.

Christopher, M., Peck, H., and Towill, D. (2006), "A Taxonomy for Selecting Global Supply Chain Strategies," *International Journal of Logistics Management,* 17(2): 277–287.

Churchill, G. A. (1979), "A Paradigm for Developing Better Measures of Marketing Constructs," *Journal of Marketing Research*, 16(1): 64-73.

Closs, D. J. and McGarrell, E. F. (2004), "Enhancing Security Throughout the Supply Chain," IBM Center for The Business of Government, Special Report Series, available at www.businessofgovernment.org.

Closs, D, Speier, C., Whipple, J., Voss, M.D. (2008), "A Framework for Protecting Your Supply Chain, *Supply Chain Management Review*, 12(2): 38-45.

Fawcett, S.E., Waller, M.A., and Bowersox, D.J. (2011), "Cinderella in the C-Suite: Conducting Influential Research to Advance the Logistics and Supply Chain Disciplines," *Journal of Business Logistics,* 32(2): 115-121.

Galbraith, C. and Schendel, D. (1983), "An Empirical Analysis of Strategy Types," *Strategic Management Journal*, 4(2): 153-173.

Hale, T. and Moberg, C. R. (2005), "Improving Supply Chain Disaster Preparedness: A Decision Process for Secure Site Selection," *International Journal of Physical Distribution and Logistics Management*, 35(3): 195-207.

Hair, J. F. Jr., Black, W. C., Babin, B. J., Anderson, R. E., and Tatham, R. L. (2006), *Multivariate Data Analysis*, 6th edition, Upper Saddle River, New Jersey: Prentice Hall.

Hawes, J.A. and Crittenden, W.F. (1984), "A Taxonomy of Competitive Retailing Strategies," *Strategic Management Journal*, 5(3): 275-287.

Helferich, O. K. and Cook, R. L. (2002), Securing The Supply Chain, Oak Brook, IL: Council of Logistics Management.

Helferich. O. K. and Cook, R. L. (2007), "Chapter 29: Global Supply Chain Security," in John Mentzer, Matthew Myers and Theodore Stank (ed.), *Handbook of Global Logistics and Supply Chain Management*, (Thousand Oaks, CA: Sage Publications, Inc.)

ISO (2007), "*Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — requirements and guidance,*" Unpublished White Paper. ISO Copyright Office, Geneva, Switzerland. Retrieved from http://www.unece.org/fileadmin/DAM/trans/bcf/news/documents/ISO28001e.pdf December 22, 2012.

Keller, S.B., Voss, M.D., and Ozment, J. (2010), "A Step Toward Defining a Customer Centric Taxonomy for Managing Logistics Personnel," *Journal of Business Logistics*, 31(2): 195-215.

Knemeyer, A. M. Corsi, T. M, and Murphy, P. R. (2003), "Logistics Outsourcing Relationships: Customer Perspectives," *Journal of Business Logistics*, 24(1): 77-109.

Landau, S. and Everett, B. S. (2004), *A Handbook of Statistical Analysis Using SPSS*, Boca Raton, FL; Chapman and Hall.

Lassar, W.M. and Kerr, J.L. (1996), "Strategy and Control in Supplier-Distributor Relationships: An Agency Perspective," *Strategic Management Journal*, 17(8): 613-632.

Lehmann, D. R. (1979), *Market Research and Analysis*, Homewood, IL: Irwin.

Lewis, A. T. (2006), "The Effects of Information Sharing, Organizational Capability, and Relationship Characteristics on Outsourcing Performance in the Supply Chain: An Empirical Study," Dissertation; The Ohio State University.

Lynch, D. E., Keller, S. B., and Ozment, J. (2000), "The Effects of Logistics Capabilities and Strategy on Firm Performance," *Journal of Business Logistics*, 21(2): 47-67.

Manuj, I. and Mentzer, J. T. (2008), "Global Supply Chain Risk Management," *Journal of Business Logistics*, 29(1): 133-56.

Martens, B. J. Crum, M. R., and Poist, R. F. (2011), "Examining Antecedents to Supply Chain Security Effectiveness: An Exploratory Study," *Journal of Business Logistics,* 32(2): 153-166.

Martha, J. and Subbakrishna, S. (2002), "Targeting a Just-In-Case Supply Chain for the Inevitable Next Disaster," *Supply Chain Management Review*, 6(5): 18-23.

Min, H. (2012), "Maritime Logistics and Supply Chain Security," In Song, D. and Panayides, P. M. (eds.) *Maritime Logistics: Contemporary Issues* (pp. 91-116) Bingley, United Kingdom: Emerald Group Publishing Limited.

Mitroff, I. I., and Alpaslan, M. C. (2003), "Preparing for Evil," *Harvard Business Review*, 81(4): 109-115.

Morgan, R. M. and Hunt, S. D. (1994), "The Commitment-Trust Theory of Relationship Marketing," *Journal of Marketing*, 58 (July): 20-38.

Netemeyer, R. G., Bearden, W. O. and Sharma, S. (2003), *Scaling Procedures: Issues and Applications*, Thousand Oaks, CA: Sage Publications.

Nunnally, J.C. and Bernstein, I.H. (1994), *Psychometric Theory* (3rd ed.), McGraw-Hill, NY.

Pagh, J. D. and Cooper, M. C. (1998), "Supply Chain Postponement and Speculation Strategies: How to Choose the Right Strategy." *Journal of Business Logistics*, 19(2): 13-33.

Quinn, F. J. (2003), "Security Matters," *Supply Chain Management Review*, 7(4): 38-45.

Reynolds, K. E. and Beatty, S. E. (1999), "A Relationship Customer Typology," *Journal of Retailing,* 75(4): 509-523.

Rice, J. B. Jr. and Spayd. P.W. (2005), "*Investing in Supply Chain Security: Collateral Benefits*," IBM Center for The Business of Government, Special Report Series. Available at www.ibm.com.

Ritchey, D. (2010), "Securing Schneider's Supply Chain," *Security*, 47(7): 50.

Sarathy, R. (2006), "Security and the Global Supply Chain," *Transportation Journal*, 45 (4): 28-1.

Scholliers, J., Toivonen, S., Permala, A., and Lahtinen, T. (2012), "A Concept for Improving the Security and Efficiency of Multimodal Supply Chains", *International Journal of Applied Logistics*, 3(2): 1-13.

Sheffi, Y. (2002), "Supply Chains and Terrorism," in *The Towers Lost and Beyond: A Collection of Essays on the WTC by Researchers at the Massachusetts Institute of Technology,* Eduardo Kausel ed, assessed on March 20th at http://web.mit.edu/civenv/wtc/

Sheffi, Y. (2005a), "Preparing for the Big One," *IEE Manufacturing Engineer*, 84(5): 12-15.

Sheffi, Y. (2005b), *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage*, Cambridge, MA: The MIT Press.

Steinman, C. (2004), "The Unfinished Agenda – Transportation Security Survey," Deloitte Services LP, Aviation and Transport Services Industry. Available at www.deloitte.com.

Tang, A. (2006), “Robust Strategies for Mitigating Supply Chain Disruptions”, *International Journal of Logistics: Research and Applications,* 9(1): 33–45.

Thibault, M., Brooks, M.R., and Button, K. J. (2006), “The Response of the U.S. Maritime Industry to the New Container Security Initiatives,” *Transportation Journal*, 45(1): 5-15.

Tokman, M., Richey, R.G., Marino, L. D, and Weaver, K. M. (2007), “Exploration, Exploitation and Satisfaction in Supply Chain Portfolio Strategy,” *Journal of Business Logistics*. 28(1): 25-57.

Trunick, P.A. (2005), “What Price Security,” *Logistics Today*, 46(8): 1-11.

Voss, M. D., Closs, D. J., Calantone, R.J., and Helferich , O. K. (2009a), “The Role of Security in the Food Supplier Selection Decision,” *The Journal of Business Logistics,* 30(1): 127-156.

Voss, M. D., Whipple, J.M., and Closs, D.J. (2009b), “The Role of Strategic Security: Internal and External Security Measures with Security Performance Implications,” *Transportation Journal*, 48(2): 5-23.

Whipple, J. M., Voss, M. D., and Closs, D. J. (2009), “Supply Chain Security Practices in the Food Industry: Do Firms Operating Globally and Domestically Differ?” *International Journal of Physical Distribution & Logistics Management*, 39(7): 574-594.

Williams, Z. (2008), “Supply Chain Security: An Institutional Approach to Strategies and Outcomes,” Dissertation; Mississippi State University.

Williams, Z., Garver, M. S., and Taylor, G. S. (2011), “Understanding Truck Driver Need-Based Segments: Creating a Strategy for Retention,” *Journal of Business Logistics,* 32(2): 194-208.

Williams, Z., Lueg, J. E, Taylor, R. D., and Cook, R. L. (2009a), “Why all the changes? An Institutional Theory Approach to Exploring the Drivers of Supply Chain Security (SCS)?” *International Journal of Physical Distribution & Logistics Management,* 39(7): 595-618.

Williams, Z., Ponder, N., and Autry, C.W. (2009b), “Supply Chain Security Culture: Measure Development and Validation” *International Journal of Logistics Management,* 20(2): 243-260.

Yang, C., and Wei, H. (2013), “The Effect of Supply Chain Security Management on Security Performance in Container Shipping Operations,” *Supply Chain Management: An International Journal*, 18(1).

AUTHOR BIOGRAPHIES

Zachary Williams is Associate Professor of Marketing and Logistics at Central Michigan University. He received a Ph.D. in Marketing at Mississippi State University. His primary research interests are in the areas of supply chain security and supply chain segmentation. E-Mail: Zac.williams@cmich.edu

Jason E. Leug is Professor of Marketing at Mississippi State University. He received a Ph.D. in Marketing at The University of Alabama. His professional experience includes positions in the banking industry in both operations/compliance and commercial lending. His research and teaching interests are in the areas of supply chain management, retailing, and strategy. E-Mail: Jlueg@cobilan.msstate.edu.

Sean P. Goffnett is Assistant Professor of Marketing and Logistics at Central Michigan University. He received his Ph.D. from Eastern Michigan University with concentration in Quality Management. His research interests include supply chain talent management, humanitarian logistics, supply chain security, leadership, process improvement and innovation. E-Mail: sean.goffnett@cmich.edu

Stephen A. LeMay is Associate Professor of Marketing at The University of West Florida. He received a DBA in Transportation at University of Tennessee, Knoxville. He has been a research, speaker, and consultant in marketing and logistics for over twenty-five years, which has primarily focused on logistics personnel. E-Mail: Slemay@uwf.edu

Robert Lorin Cook is Professor of Marketing and Logistics at Central Michigan University. He received a Ph.D. in Marketing at Michigan State University. His primary research interests are in the areas of supply chain design, applying information system technologies to logistics systems and logistics education. E-Mail: Robert.cook@cmich.edu