ISSN: 1545-679X

Information Systems Education Journal

Volume 7, Number 76 http://isedj.org/7/76/ July 14, 2009

In this issue:

Improving the Global Supply Chain through Tightening Information Technology Security

Kamal M. Kakish
Lawrence Technological University
Southfield, MI 48075 USA

Abstract: Automotive Global Supply Chain (GSC) trade and transport is very complex. It involves multiple players and a gigantic number of complex transactions. Consequently, there is a constant need to obtain, analyze, and exchange data securely and compliantly. The rapid changes in Information Technologies coupled with political and socio-economic factors are continuously transforming international trade and transport operations. The importance of GSC IT security and trade compliance has been emphasized increasingly in recent months (ex: WCO SAFE Framework(TM) Data Model). Given these challenges, this doctoral research analyzed the dynamics and provided a conceptual solution model that could potentially improve IT security and compliance levels globally. The literature review showed that a significant portion of processing GSC documents in the automotive industry is still paper-based. This causes significant transport delays and increases the potential for errors and IT security exposures. The conceptual model involves establishing a GSC Hosted IT Security Infrastructure Framework coupled with a GSC IT Security Policy that aligns and interoperates with UN Recommendation 33 and the WCO Data Model. The study sought to explain strategic issues related to IT management and industry participants behavior. The study used a mixed-methods descriptive research design using a questionnaire and a set of interviews as the primary means of data collection. The interviews covered a comprehensive representation of global Industry participants. The results of this research demonstrated a statistical correlation between IT Security and trade compliance. These results are beneficial to GSC IT Security administrators, technical, and operational specialists.

Keywords: Global Supply Chain (GSC), IT Security, Hosted IT Services, Secure Electronic Transport

---

Recommended Citation: Kakish (2009). Improving the Global Supply Chain through Tightening Information Technology Security. *Information Systems Education Journal, 7* (76). http://isedj.org/7/76/. ISSN: 1545-679X. (A preliminary version appears in *The Proceedings of ISECON 2007:* §3153. ISSN: 1542-7382.)

This issue is on the Internet at **http://isedj.org/7/76/**

The **Information Systems Education Journal** (ISEDJ) is a peer-reviewed academic journal published by the Education Special Interest Group (EDSIG) of the Association of Information Technology Professionals (AITP, Chicago, Illinois). • ISSN: 1545-679X. • First issue: 8 Sep 2003. • Title: Information Systems Education Journal. Variants: IS Education Journal; ISEDJ. • Physical format: online. • Publishing frequency: irregular; as each article is approved, it is published immediately and constitutes a complete separate issue of the current volume. • Single issue price: free. • Subscription address: subscribe@isedj.org. • Subscription price: free. • Electronic access: http://isedj.org/ • Contact person: Don Colton (editor@isedj.org)

This paper was selected for inclusion in the journal as part of the ISECON 2007 best papers group. Best papers received preliminary reviews by three or more peers placing them in the top 30% of papers submitted and final reviews placing them in the top 15% by three or more former best papers authors who did not submit a paper in 2007.

EDSIG activities include the publication of ISEDJ and JISAR, the organization and execution of the annual ISECON and CONISAR conferences held each fall, the publication of the Journal of Information Systems Education (JISE), and the designation and honoring of an IS Educator of the Year. • The Foundation for Information Technology Education has been the key sponsor of ISECON over the years. • The Association for Information Technology Professionals (AITP) provides the corporate umbrella under which EDSIG operates.

Improving the Global Supply Chain through Tightening Information Technology Security

Kamal M. Kakish
profkakish@gmail.com
College of Management, Lawrence Technological University
Southfield, MI 48075, USA

ABSTRACT

Automotive Global Supply Chain (GSC) trade and transport is very complex. It involves multiple players and a gigantic number of complex transactions. Consequently, there is a constant need to obtain, analyze, and exchange data securely and compliantly. The rapid changes in Information Technologies coupled with political and socio-economic factors are continuously transforming international trade and transport operations. The importance of GSC IT security and trade compliance has been emphasized increasingly in recent months (ex: WCO SAFE Framework™ Data Model). Given these challenges, this doctoral research analyzed the dynamics and provided a conceptual solution model that could potentially improve IT security and compliance levels globally. The literature review showed that a significant portion of processing GSC documents in the automotive industry is still paper-based. This causes significant transport delays and increases the potential for errors and IT security exposures. The conceptual model involves establishing a GSC Hosted IT Security Infrastructure Framework coupled with a GSC IT Security Policy that aligns and interoperates with UN Recommendation 33 and the WCO Data Model. The study sought to explain strategic issues related to IT management and industry participants behavior. The study used a mixed-methods descriptive research design using a questionnaire and a set of interviews as the primary means of data collection. The interviews covered a comprehensive representation of global Industry participants. The results of this research demonstrated a statistical correlation between IT Security and trade compliance. These results are beneficial to GSC IT Security administrators, technical, and operational specialists.

Keywords: Global Supply Chain, GSC, IT Security, Hosted IT Services, Secure Electronic Transport

1. INTRODUCTION

Automotive Global Supply Chain (GSC) trade and transport is very complex. It involves multiple players (AKA Industry Participants – IP's) and a very large number of multifaceted transactions. A typical automotive trade business deal may easily involve 30 parties, 40 documents, 200 data elements, and require re-encoding of 60 to 70 per cent of all data at least once. Potential exploits abound. Consequently, there is a constant need to obtain, analyze, and exchange data securely and compliantly.

The rapid changes in Information Technologies (IT) coupled with political and socio-economic factors are continuously transforming international trade and transport operations. In the last few months, governments and business organizations have increasingly emphasized the importance of supply chain security and trade compliance (Neef et al., 2004). This is evidenced by the recent wide adoption of the World Customs Organization (WCO) Framework of Standards to Secure and Facilitate Global Trade (SAFE Framework).

Benefits of conducting this study may contribute to improvements for solving end-to-end shipment data visibility, supply chain goods security, data security, and potentially interoperability issues. Whenever measurable benefits can be gained in the Automotive GSC, based upon this research effort, a

focused interest by government and industry executive management promotes widening the topic's knowledge to maximize such benefits. Additionally the impact of the GSC on the global economy, makes the importance of this research study compelling.

This paper focuses on the improvement of IT security and trade compliance in the GSC. The research project sought to explain strategic issues related to the behavior of IT management and automotive IP's. An inductive-hypothetic research strategy supported by mixed methods was adopted, and is summarized in the research design section.

The results of the research literature review, questionnaire, and interviews implied that IT security and trade compliance are almost non-existing among many developing country SME's and that a GSC IT Security Policy is necessary to improve IT security and trade compliance.

The paper is structured in the following sections: Research Problem; Research Objectives; Research Design; Importance of GSC IT Security; Significance of Compliance with GSC IT Security; Challenges of IT Security and Compliance in the GSC; Compliance Challenges; The Conceptual Solution; Interviews and Questionnaire; Data Analysis and Validation; and future directions. The paper ends with a summary and provides some conclusions.

Research Problem

Processing and tracking shipment containers across long distances suffers significant problems throughout the world. Such inefficiencies include substantial delays in moving freight, missing critical information, limited end-to-end shipment visibility, split shipments and disruption, but chief of all is the wide exposure to disasters, natural and otherwise, due to the lack of robust information security mechanisms (Caballero, 2005; Katz, 2004). Clearly, these issues translate into significant increases in cost and deficient shipment visibility – a business loss that can be avoided. These dynamics further complicate the ability of automotive industry participants to comply and operate efficiently and securely within the GSC.

Given these situations and challenges, a research project was undertaken to analyze the dynamics of IT Security within the automotive GSC. The research analysis yielded a conceptual solution (AKA the conceptual model). The objective of the GSC IT security conceptual model is two-fold: 1) contribute toward improving the IT security of data exchange, and 2) improve the trade compliance levels of Small-to-Mid Enterprises (SME's) and their suppliers in developing countries.

Research Objectives

The objectives of this research are to:

1. Improve Overall GSC IT Security.
2. Simplify global Compliance (C-TPAT, WCO Standards for Secure Trade, etc).
3. Improve information messaging security of the Global Automotive Supply Chain.
4. Improve GSC Data Transaction Security regardless of data types and messaging methods.
5. Increase the efficiency of GSC end-to-end Data Exchange.
6. Enable/empower developing countries Small-to-Midsize-Enterprises and Joint Ventures to compete globally and trade securely.

Research Design

The study used a mixed methods descriptive research design using a questionnaire and a set of interviews as the primary means of data collection. The objectives of the interviews were to validate and improve the prototyped (by way of models) GSC IT Security conceptual model. The interviews covered a wide representation of Industry participants from the US government, United Nations, WCO, NIST, technology providers, OEM's, and Tier-1 suppliers. The questionnaire used over 50 yes/no/unsure questions covering strategic IT related categories, including IT strategy, IT governance, IT integration, procurement, quality, IT security and trade compliance.

In order to formulate a research strategy, one needs to understand the problems and their sources, and then determine how to investigate and solve these problems. According to Sol (1988), the research problem represents an ill-structured problem. The researcher creates an image of reality and this raises questions and imposes requirements on the research approach.

The research strategy concerns the steps that are carried out to execute the inquiry

into the phenomenon studied, and it consists of an outline of the sequence of data acquisition and analysis required to do the research at hand (Vreede, 1995). In this research, the researcher followed the inductive-hypothetic research strategy, depicted in Figure 3, as it is applicable to this type of research. This strategy consists of five steps (Churchman, 1971; Sol, 1982; Vreede, 1995; Laere, 2003):

1. **Initiation**: using a number of undeveloped theories, some empirical situations are described.
2. **Abstraction**: the essential aspects are abstracted into a conceptual model.
3. **Theory formulation**: using the descriptive model, a prescriptive conceptual model is derived in the form of a theory.
4. **Implementation**: test the theory by implementing the model in one or more prescriptive empirical situations.
5. **Evaluation**: the results of the prescriptive empirical situations are evaluated.

The concept of "theory formulation" in the research strategy is used in a broad sense. It indicates an explicit and elaborated set of solutions for the original problem statement (Meel, 1994).

The following benefits could be obtained by following this research strategy (Sol, 1982; Meel, 1994):

1. Emphasis on the specification and testing of premises in an inductive way.
2. Opening up possibilities for a problem specification using an interdisciplinary approach.
3. Enabling the generation of various alternatives for the solution of the problem.
4. Permitting learning by regarding the analysis and synthesis as interdependent activities.

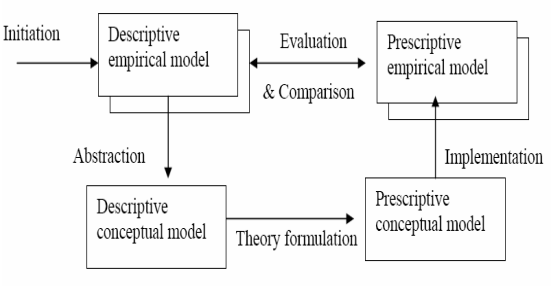

Figure 1: The Inductive-Hypothetic Research Strategy

These benefits make the inductive-hypothetic research strategy very useful for new and emerging research fields such as GSC IT Security improvement.

In addition, the research adopted a variety of tools and frameworks in order to build the conceptual solution model. These include Class Diagrams using UML 2.0 notation, Rummler-Brache Performance Matrixes, information analysis, requirement analysis, gap analysis, design principles, strategy hierarchy, openness scale, organizational influence, project initiation framework, levels of conformance and many more[i].

2. IMPORTANCE OF GSC IT SECURITY

Global supply chain serves as the backbone for international trade, which is an essential driver for economic prosperity and socio-economic development throughout the world. Today's global trading system is vulnerable to a variety of IT security exploitations that could severely damage the entire global economy (Dresser et al., 2004). While government organizations strive to control and administer the international movement of goods, real evidence dictates that there exists dire need to provide increased electronic IT security to the global supply chain.

To gain a better appreciation of the magnitude of these issues, one needs to understand the underlying processes, governances, technologies, tools, and techniques associated with global supply chain inventory and freight management. However, the scope of this research effort focused only on the element of information technology, particularly as relevant to automotive GSC data security.

A variety of strategies, initiatives, and Internet-based materials and inventory tracking technology types are continually being integrated into supply chain management systems (Christopher, 2005). International governments and businesses, as well as world trade and customs organizations have recently taken significant stride in establishing and implementing global standards and technologies in the quest of addressing various security exposures of the global supply chain (Simchi-Levi et al., 2004). These organizations include the World Customs Organization (WCO) with its Framework of Standards to Secure and Facilitate Global

Trade, U.S. Customs and Boarder Protection with its Customs Trade Partnership Against Terrorism (C-TPAT) initiative, World Trade Organization (WTO), United Nations (UN) with Recommendation 33, and the European Union. These organizations along with several other countries have committed to developing global trade implementation guidelines.

A 2005 AMR Research study (AMR Research, 2005) concluded that:

91% of automotive industry participants still use manual procedures to correct shipments, and to communicate status and visibility.

15% of shipments experience delays due to inaccurate or incomplete data.

79% believe standardizing "exchange of information" will reduce disruptions in supply chain.

87% believe improvement in long distance supply chains is needed.

Recurring problems involving the extensive use of paper documents, emails and faxes significantly effect these complex material movements. The paper document trail results in compliance problems, data quality deficiencies, shipment visibility deficiencies, and causes avoidable delays and the expenditure of additional resources for problem resolution.

3. SIGNIFICANCE OF COMPLIANCE WITH GSC IT SECURITY

In today's highly regulated environment, trade compliance is a daunting challenge to organizations because they face a mountain of regulatory obligations. Compliance is a process that involves policy, people, process, and technology. In the past, organizations tackled compliance as islands of projects scattered throughout the organization, leading to inconsistent approaches and a duplication of efforts (US General Accounting Office, et al., 2004).

The common trend among many IT security technology providers has recently revealed a special interest and an increased focus on the security of supply chain information exchange (Neef et al., 2004). For example, VeriSign™, one of the prominent global IT security technology providers recently announced the acquisition of Retail Solutions Inc, and a partnership with the WorldWide Retail Exchange™ (WWRE) (Connaughton, 2006). This demonstrates significant interest within the IT security industry to extend their products and services deep into the global supply chain.

Several IT vendors claim to have the answers for the compliance and IT security problems that most midsize organizations in the developing world face. However, most of these vendors provide capabilities to meet only a single requirement or a handful of requirements and really are not a security and compliance management vendor themselves. Real IT security and compliance vendors are those who provide a platform for documenting and overseeing security and compliance across a developing world organization such as Small to Medium Enterprises (SME's), US Tier-1 organizations, and the GSC as a whole.

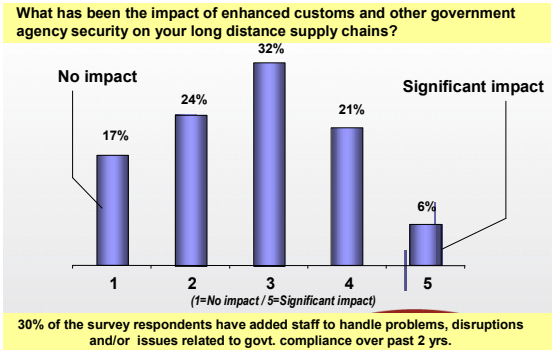

Figure 2: Impact of Compliance on IT

A 2007 report by the Automotive Industry Action Group (AIAG) Material Off-Shore Sourcing - MOSS project showed that compliance affected the IT organization budget and resources. Figure 2 demonstrates this impact.

Security spending has steadily risen over the past few years to become a significant percentage of the corporate budgets. Up until recently, senior executives had given free reign to security mangers due to compliance initiatives. Nevertheless, most organizations are over the hump of initial spending on compliance, and senior executives want to know where the money is being spent — to judge whether benefits are worth the expense.

To achieve sustainable compliance, firms must develop a process and management

function. In line with government guidance, sustainable trade and data security compliance must encompass and sustain best compliance practices that include the following steps:

1. Document the policy and control environment.
2. Assign appropriate oversight of compliance management.
3. Require personnel screening and access control.
4. Ensure compliance through training and communication.
5. Implement regular control monitoring and auditing.
6. Consistently enforce the control environment.
7. Prevent and respond to incidents and gaps in controls.

Organizations that do not embrace compliance management as a defined business process will approach compliance as fragmented projects, trying to sneak past the regulators' gaze (Kagami et al., 2004). This minimalist mindset may appear to work for a short time; however, it is a recipe for disaster because no specific oversight compliance is in place.

In today's dynamic business environment, gaps quickly arise that can push an organization out of compliance. IT systems, employees, relationships, and compliance requirements have changed; ultimately, business has changed. In addition, no one has managed compliance accordingly. Furthermore, when regulators come asking questions and there is no central person ready to answer them, the organization looks confused and unorganized and will receive more scrutiny.

4. CHALLENGES OF IT SECURITY AND COMPLIANCE IN THE GSC

There is no shortage of specifications, standards, methods, and tools at any level within the GSC. There's an abundance of international standards, specifications, control frameworks, harmonization concepts (ex: Single Window Facilitation), and recommendations as evidenced by the wealth of trade publications from diverse organizations. These include but are not limited to the UN, WCO, WTO, IMO, ICC, ICC/UNCTAD, COBIT, NIST, ISO, FFIEC, DHS (C-TPAT), industry associations (AIAG, APQC), and several others. While such an abundance of standards and recommendations may be beneficial, overall they present significant challenges to the Industry Partners. These challenges include inconsistency, incompatibility, implementation requirements, and a lack of enforcement.

The challenge for IT Security Managers is to not only identify what is important but also to be able to tie this information from disparate tools into business-centric metrics so that the senior executives can understand them, take action, and be confident that the enterprise is secure.

Over the past five years, the GSC has seen a dramatic increase in trade-information requirements. The chief causes of such an increase are the convolution of the supply chains, the number of parties involved, and the speed at which goods are exchanged.

Over the last several years, there has been a flood of regulations mandating information security. Soon after 9/11, the US government formed the Department of Homeland Security (DHS) and US Customs and Border Protection (CBP) among others. Consequently, several agencies consolidated under the new department's jurisdiction. Given their new homeland security mandate at the borders, CBP created C-TPAT and published suggested security guidelines for importers to implement supply chain security in order to reduce the risk of terrorists and weapons of mass destruction penetrating the US homeland via importing conveyances (DHS, 2007).

The US government also imposed stringent security measures, including Advance Cargo Information (ACI), Container Security Initiative (CSI), and Customs-Trade Partnership Against Terrorism (C-TPAT) (DHS, 2007). Each one of these initiatives depends heavily on reliable, structured, and sophisticated information on the trade transaction. Using automated risk assessment procedures, they profoundly analyze the electronic information provided. As such, it is becoming increasingly obvious that by adopting more electronic-based (and less paper-based) trades, organizations and governments can comply more fully with trade procedures, conduct more accurate risk analysis, and thus make the GSC more efficient and secure.

Accordingly, other countries began to follow suit: Canada with its Partners in Protection (PIP) and Mexico studying a similar program. In March 2005, CBP began to change its C-TPAT recommendations to risk based "criteria" so it can be implemented based on risk assessments of supply chains. It also published criteria for other parties participating in the supply chain. In addition, the World Customs Organization also studied the issue of supply chain security and in June 2005 published WCO Framework of Standards to Secure and Facilitate Global Trade (SAFE).

One might argue that the creation of additional regulations compounds the cycle of data exchange and collaboration complexity, thereby slowing the process of global data transaction messaging and affecting the funds and resources that were once available to IT security purposes. Clearly, there is a need to build an effective strategy to deal with compliance issues. Participants in the automotive global supply chain should determine the requirements of all the various regulations covering corporate governance, privacy, risk management, information integrity, and identity theft among others.

To complicate this picture further, organizations are advised to use control frameworks and/or standards such as COBIT, NIST, ISO 17799, FFIEC and many more. These all share common information security controls in risk management, authentication, access control, data protection, logging, and reporting. For some regulations, governments recommend a particular control framework or standard while other regulations leave it up to industry to decide which set of controls to use.

Determining specific requirements can be difficult. Most automotive organizations face multiple regulations and will have to consider multiple control frameworks (Cranor et al., 2003). Moreover, many of these frameworks and standards reference each other, adopt each other, and in some cases can be outdated.

Compliance Challenges

Today's GSC business environments present additional challenges and constraints to the IT Security Compliance processes:

1. Lack of Unified/Common GSC IT Security Policy.
2. Lack of defined processes for maintaining and keeping IT security, privacy, and other related business controls current and updated.
   a. Without a defined process for maintaining and keeping controls up to date, GSC IPs will find that many of their controls will soon be "non-compliant" due to normal changes in their business and IT environments.
3. Continuous expansion and change in:
   a. IT Security Technologies (a quick look at RFID makes this obvious).
   b. Business boundaries, audit requirements (just consider Sarbanes-Oxley), and other factors.
   c. Local and international IT Security Policies.
4. New technology brings new risks, new processes and thus new compliance issues.
5. Lack of flexibility - GSC enterprises need flexibility to remain competitive.
   a. Rigid control processes can hinder flexibility, thus hurt GSC IP business's ability to operate effectively.

Clearly, the automotive industry today suffers from a multitude of issues related to the security, accuracy, and timely availability of supply chain information. A number of recent studies have shown that electronic security of automotive data transactions remains a chief contributor to the inefficiencies with the automotive Global Supply Chain (Benson et al., 2005; Sichel et al., 2005; Willis et al., 2004). Considering the volume of automotive global trade transactions, the high profile of the automotive industry and scrutiny given to automotive global shipments, secure and timely information is key to the success and continued advancement of the industry and its participants.

5. CONCEPTUAL SOLUTION

The ultimate purpose of the conceptual model is to facilitate secure and efficient GSC data exchange through dynamic maintenance of a global IT Security Policy, ensuring IP trade compliance, and providing tools that enable linkage and possible integration with the existing ERP and SCM systems.

In order to conceptualize the solution, the researcher has relied on a variety of models

and meta-models, assumptions, approaches, and techniques. Such artifacts include Criteria for Adoption (including Technology Selection Criteria), Demonstration of Concept, Focal Theory, Background Theory, and other relevant solution conceptualization factors (Creswell, 2003).

A key criterion of the conceptual solution is strict compliance to US and international export/import laws and regulations (WCO compliance). At a minimum, the solution should offer innovative and proven methods for promoting IT security according to specified criteria for exchanging data over networks across the globe.

When building a highly effective compliance and security program, one needs to keep in mind that the process involves policy, people, process, and technology. Policies provide the governance for controls and define the expected ethical and compliant behavior. Furthermore, while policies are part of the documentation in the first habit, they permeate all of the other habits, providing the behavioral foundation for each of them. Therefore, organizations must ensure that policies are well defined and understood because without this effort, all else fails (Doukidis et al., 2005).

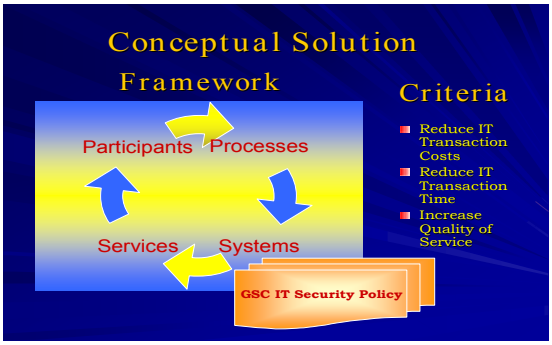

Figure 3: GSC IT Security Conceptual Model Framework

Ultimately, compliance violations come down to people. Whether malicious or accidental, the people element introduces uncertainty into the compliance process. Effective compliance program managers focus on developing a culture of compliance in which individuals behave ethically and responsibly. Achieving effective compliance requires ongoing compliance processes. Organizations should avoid compliance islands and aim for consistency by approaching compliance as a process as opposed to individual projects (Gupta et al., 2004).

The GSC Hosted IT Security Services Conceptual Model Framework, shown in Figure 3, is comprised of the following components:

1. Industry Organizations (AKA Industry Participants or IP's) - These include: OEMs (in this scenario OEMs equal US Tier-1 suppliers), Developing World Suppliers (in this case these are known as Small-to-Midsize Enterprises - SMEs), customers, World Organizations (ex: WCO, WTO, UN, etc), Regulators (ex: International Governments, US Federal Government agencies), Technology Providers (IBM, Oracle, Microsoft, etc), Carriers, Financial and Insurance Services, e-Business/e-Commerce industry marketplaces and exchanges (ex: COVISINT), retailers, and consumers.
2. Processes - A set of processes which are based on regulatory and business objectives and defined and agreed upon by all major industry participants. Such processes drive standards that simplify infrastructure, and provide for common means communication, interoperability, and data exchange. Standards result in quicker implementations with reduced variables. For technology providers, standards development provides a competitive advantage by building knowledge about cross-industry and intra-industry drivers, and developing products and services accordingly.
3. Systems - Technologies designed and implemented in terms of web-based software systems and tools. These web-based systems will leverage a variety of tools and technologies including web servers, network and communication servers, IT security and policy servers (for authentication and compliance), and software application servers for integration with existing ERP and SCM systems. Figure 4 illustrates the technology relationship with the other components of the conceptual solution in terms of a **meta-model** framework. These technologies should enable the industry participants to access automotive transaction data forward-and-backward providing secured visibility throughout the GSC.
4. Services – These include a range of support activities that enable the trading

partners to exchange data securely and assure compliance of the SMEs in developing countries. These services will work to satisfy the pre-determined criteria of: a) reducing IT transaction costs; b) reducing IT transaction time; and c) increasing the Quality of Service, as shown in Figure 3. Examples of these services should manifest the ability of Teir-1 suppliers in the US to present their purchasing needs to a much larger base of compliant SME's throughout the world. Equally, the same services could enable developing country suppliers to compete legitimately at a global level.

The combination of the components above, working together comprises the entire conceptual solution.

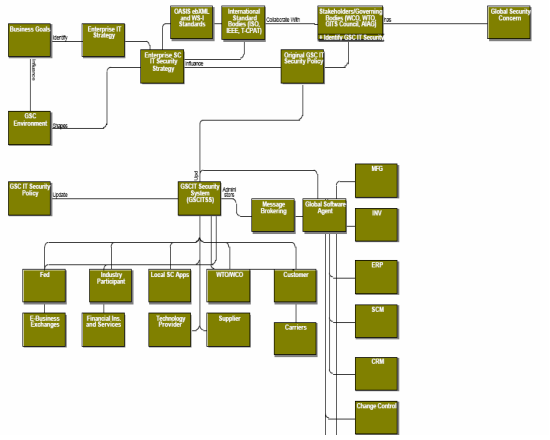

Figure 4: GSC IT Security Meta Model

The dynamics of the conceptual solution can be seen in Figure 5. While this figure shows data exchange between an OEM and a Tier-1 supplier, it could also illustrate collaboration among any two or more industry participants. The mechanisms for the activities in Figure 5 operate as follows:

1. Suppliers can connect to the Global Supply Chain IT Security System (GSCITSS) server using a variety of methods. GSCITSS will supply the necessary authentication to enable data transaction security and collaboration.
2. Transaction data, which is securely transported from the Supplier to GSCITSS, could be mirrored in several locations across the globe.
3. Transaction Data travels securely from the GSCITSS server to the OEM (or other IP) production server, still compliant, encrypted, and packaged. The OEM server transports periodically (every 10 minutes) transaction data to/from GSCITSS server.
4. Transaction Data travels securely from the OEM or IP production server to the OEM/IP Data Managers. The secure data is then routed to an OEM or IP user a specific pre-destined OEM/IP location.
5. The process can initiated from either end. Transaction traceability is always available to both ends.

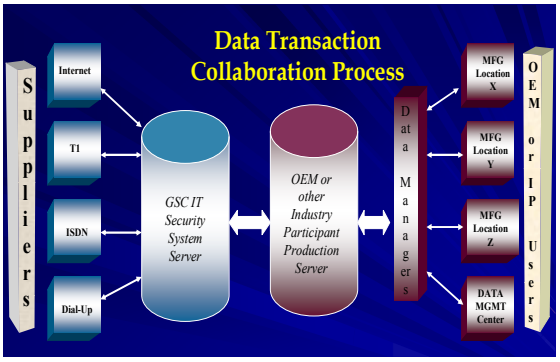

Figure 5: Data Transaction Collaboration Process

6. INTERVIEWS AND QUESTIONNAIRE

The primary method of collecting data for this research relied heavily on conducting interviews and questionnaires with a comprehensive representation of the GSC IT Security and Compliance industry members.

The process of identifying the interviewees required prior approval by the dissertation committee and the research advisor. The interviews covered a wide representation of Industry participants from the US government, United Nations, WCO, NIST, technology providers, OEM's, and Tier-1 suppliers. The ultimate objective of conducting the interviews sought to validate the soundness and applicability of prototyping and eventually implementing the conceptual solution. Therefore, analysis results of the answers provided by the interviewees were processed for this purpose. Additional interviewee answers sought to explain behavioral issues related to GSC IT Security and global (WCO based) compliance (WCO, 2007) Eleven (11) interviews were conducted over a period of 8 weeks, involving over 20 supply chain professionals and IT executives (Snack et al., 2007), using a variety of collaboration methods, and in various locations. Appendix

A provides a Table which represents the organizations that were interviewed and answered the questionnaire[ii].

Prior to conducting the interviews, four documents were made available to each interviewee[iii]:

- An Abstract of the research.
- An Overview of the Interview - around 30 pages of research and interview details.
- The Questionnaire.
- The PowerPoint presentation used during the interview .

The interviews lasted from 45 minutes to 3 hours. While one-half of the interviews were conducted in person, the other half was conducted using WebEx™ conferencing technology.

The interviews started by presenting a PowerPoint presentation that identified the research objectives, reviewed the GSC IT Security and Compliance issues and challenges, then overviewed the conceptual solution. Questions that were asked during the interview are shown in Appendix B.

After facilitating a brief period of Q&A, the interviewees were asked to *validate* the conceptual model and indicate their acceptance and/or support of implementing and/or prototyping such a solution.

The interviews ended with asking the interviewees to follow-up with the researcher with any questions, concerns, or suggestions.

The questionnaire was given to the interviewees prior to conducting the interview. It contained a checklist of over 50 yes/no/unsure questions that cover strategic enterprise IT security issues. The strategic IT related categories include strategy, governance, integration, procurement, quality, and security. The purpose of the questionnaire is to obtain an understanding of the GSC IT Security issues in the Automotive Industry as they relate to a number of enterprise strategic issues.

The questionnaire[iv] is based on Col Perks and Tony Beveridge's Management Checklist (Perks et al., 2003). It is intended to be used as a mean of identifying the current state of IT security within the global supply chain.

7. DATA ANALYSIS AND VALIDATION

The analysis given here is intended as an example to demonstrate how the data analysis was designed and carried out. The actual findings of the complete data analysis are discussed in Chapter 4 of the Dissertation, which is not included here. Table 1 contains a portion of the raw data that was collected from the answers to the strategic IT related business areas of the questionnaire. Specifically, the table shows the raw data of the two strategic areas: *IT Security and Trade Compliance*. This data shows the relationship for comparison and observation purposes, for these various strategic IT related business areas that were asked of the interviewees via the questionnaire.

A quick review of Table 1 shows that the "Interview #" column of the spreadsheet shown below corresponds to number associated with the Interviewee Organizations table of the dissertation document. For example, Interview number 1 is AAM, #2 is GM, and so on. In addition, there are five questions for the security ranking, with possible answers (Y, N, and U). A "No" answer for security means that the organization interviewed is doing well, and does not suffer significant problems with the security of their electronic data. Therefore, we rank the number of "No's" for security as this: 5 is highest, 0 is lowest. For the compliance ranking, 5 questions were asked in the questionnaire. Positive answer range from 3 to 5 and negative answers include 1 and 2. Therefore, a "Yes" answer for compliance means that the organization interviewed is compliant.

Security and Compliance						
	Security			Compliance		
Interview #	Y	N	U	Y	N	U
1	1	4	0	5	0	0
2	1	4	0	4	1	0
3	0	3	2	2	0	0
4	2	2	1	1	1	0
5	0	4	1	4	1	0
6	0	5	0	4	1	0
7	1	4	0	5	0	0
8	0	5	0	5	0	0
9	0	4	1	4	1	0
10	1	3	1	3	2	0
11	1	4	0	4	1	0

Table 1: Raw Questionnaire Data for Security & Compliance

Upon plotting the "No" answers of Security with the "Yes" answers of Compliance in MS Excel™ in a XY Scatter Chart, we obtain the fitted line shown in Figure 6, with a coefficient of determination R^2 = 0.7234.

In essence, it is observed that a high statistical correlation exists between IT Security and Trade Compliance among the 11 organizations interviewed. This correlation suggests that the more IT secure an organization is the more trade compliant it is, and vice versa.

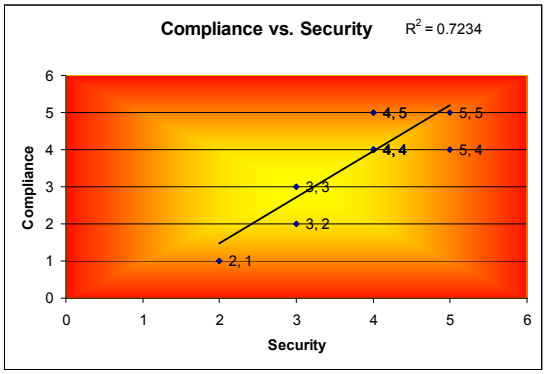

Figure 6: Using Least Square Method to Correlate Security & Compliance

Additional analysis of the interview and questionnaire answers were performed for other categories such as IT strategy, IT governance, IT integration, Quality, Procurement, IT Security and Compliance.

Some of these observations and findings were easily seen by performing simple investigation of the raw data and reviewing the feedback from the interviews. At the highest level, these findings seemed to confirm the hypothesis of this research in the following observations:

1. Most USA-initiated data exchange transactions are electronically secure, given adequate implementation of SCM systems and technology infrastructure.
2. IT security of developing world countries data transactions is largely driven by USA OEMs and Suppliers.
3. Compliance is almost non-existing among most developing country SME's.
4. A Global Supply Chain IT Security Policy is necessary to improve compliance and tighten electronic security. improve compliance.

The results also demonstrated a statistical correlation between IT Security and trade compliance.

8. FUTURE DIRECTIONS

Undertaking a global level IT research of this magnitude may prove to be a complex and daunting task. However, given adequate funding and support (in terms of corporate sponsorship of a large-scale prototype), it remains to be reasonably possible to advance the improvement of IT security and compliance within the GSC.

This effort has barely scratched the tip of the iceberg in terms of identifying the GSC IT security and compliance problems, and proposing a robust conceptual model that when implemented globally could achieve the desired improvement.

Conducting the interviews with a comprehensive representation of the industry's IT Security and GSC executives made it clear that such an implementation is possible and within reach. The greatest majority of the interviewees validated the conceptual solution positively and indicated interest in supporting the implementation of a prototype by their willingness to participate in a pilot and by funding the implementation.

A logical next step would be to design and implement a prototype across the globe. One of the most effective areas of implementing the conceptual solution prototype would be on top of existing UN Single Window Facilitation® implementation (United Nations, 2007), where the IT infrastructure is already available and operational. A follow-on to the UN Single Window implementations could include expanding the prototype to developing countries' SMEs.

Ultimately, a full-fledge implementation of the conceptual solution model could be implemented across the globe and administered and regulated via international organizations such as the WCO, the UN, and the WTO.

9. CONCLUSION

Complexities in the Automotive GSC cause several entities to experience and tolerate compliance and electronic information security pressures. This research was conducted with emphasis on IT management and IP's

behavior was instrumental in identifying potential improvements to supply chain information security. The researcher defined the problems and challenges facing the electronic GSC, and devised a conceptual solution to mitigate the risks of these problems. To validate the conceptual solution, the researcher interviewed with eleven industry representative organizations and 21 individuals. Upon careful analysis of the data, it became apparent that by adapting a systematic approach to data exchange, industry participants could promote the security of information and data sets across the automotive global supply chain.

The literature review showed that a significant portion of processing GSC documents in the automotive industry is still paper based. This causes significant transport delays and increases the potential for errors and IT security exposures. The conceptual model presented by this research could eliminate this paper based processing by establishing a GSC Web Hosted IT Security Infrastructure Framework coupled with a GSC IT Security Policy that aligns and interoperates with UN Recommendation 33 and the WCO Data Model.

The study provided an in-depth analysis of the strategic issues related to Automotive GSC IT management and IP's behavior. The results of this study demonstrated a statistical correlation between IT Security and trade compliance. These results are beneficial to GSC IT Security administrators, technical, and operational specialists when making decisions about technologies that affect the GSC electronic transport process as well as assist in automotive industry decision making regarding where to commit resources.

10. REFERENCES

Benson, A. S., Massachusetts Institute of Technology. (2005). The role of organizational culture in creating secure and resilient supply chains.

Caballero, C. G., Sloan School of Management, Massachusetts Institute of Technology Dept. of Mechanical Engineering & Leaders for Manufacturing Program, (2005), Leading a lean transformation in the wake of a disaster, Boston, Mass.

Christopher, M. (2005). Logistics and supply chain management : creating value-added networks (3rd ed.). Harlow, England ; New York: Financial Times Prentice Hall.

Connaughton, P. (2006). Supply Chain Management. Forrester Research.

Cranor, L. F., & Wildman, S. S. (2003). Rethinking rights and regulations : institutional responses to new communication technologies. Cambridge, Mass.: MIT Press.

Creswell, J. W. (2003). Research design : qualitative, quantitative, and mixed methods approaches (2nd ed.). Thousand Oaks, Calif.: Sage Publications.

DHS - Department of Homeland Security, (2007), Comprehensive Security National Strategy, retrieved from: http://homelandsecurity.ohio.gov/

Dresser, E. L., & Massachusetts Institute of Technology. Dept. of Ocean Engineering. (2004). The effectiveness and economic impact of enhancing container security. Unpublished Thesis S.M. --Massachusetts Institute of Technology Dept. of Ocean Engineering 2004.

Doukidis, G. I., & Vrechopoulos, A. P. (2005). Consumer driven electronic transformation : applying new technologies to enthuse consumers and transform the supply chain. Berlin ; New York, NY: Springer.

Gupta, J. N. D., & Sharma, S. K. (2004). Intelligent enterprises of the 21st century. Hershey, PA: Idea Group Pub.

Kagami, M., Tsuji, M., & Giovannetti, E. (2004). Information technology policy and the digital divide : lessons for developing countries. Cheltenham, UK ; Northhampton, MA: Edward Elgar.

Katz, R., (2004), The human side of managing technological innovation: a collection of readings, (2nd ed.), New York: Oxford University Press.

Neef, D., & NetLibrary Inc. (2004). The supply chain imperative (1st ed.). New York: American Management Association.

Perks, C., & Beveridge, T. (2003). Guide to enterprise IT architecture. New York: Springer-Verlag.

Sichel, A. R., & Massachusetts Institute of Technology. Dept. of Ocean Engineering.

(2005). Supply chain security along the Columbia River

Simchi-Levi, D., Kaminsky, P., & Simchi-Levi, E. (2004). Managing the supply chain : the definitive guide for the business professional. New York: McGraw-Hill.

Snack, P., and Kakish, K., (2007). Snack-Kakish DMIT Dissertation Interviewee List.

United States General Accounting Office & United States Office of Compliance, (2004), Office of Compliance status of management control efforts to improve effectiveness: report to congressional committees, retrieved from http://purl.access.gpo.gov/GPO/LPS52554

United States Government Accountability Office, (2006), Cargo Container Inspections: Preliminary Observations on the Status of Efforts to Improve the Automated Targeting System.

WCO, (2007), World Customs Organization. The WCO Data Model. Retrieved from http://www.wcoomd.org/ie/EN/Topics_Issues/FacilitationCustomsProcedures/facil_wco_data_model.htm

Willis, H. H., & Ortiz, D. (2004). Evaluating the security of the global containerized supply chain. Santa Monica, Calif.: RAND Corporation.

Appendix A

#	Organization Type & Name	Description of Business
1	Supplier AAM	American Axle and Manufacturing is a 4.5 billion dollar business that specializes in manufacturing Gears and Axles. www.aam.com
2	OEM GM	General Motors is the largest OEM in the world. www.gm.com
3	Standards Body NIST	The US National Institute of Standards and Technology mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. http://www.nist.gov/
4	Supplier Federal Mogul	Federal-Mogul Corporation is an innovative and diversified $6.3 billion global supplier of quality products, trusted brands and creative solutions to the automotive, light commercial, heavy-duty truck, off-highway, agricultural, marine, rail and industrial markets. The 45,000 people of Federal-Mogul located in 35 countries and drive excellence in all they do. http://www.federal-mogul.com/en
5	US Government DHS	Homeland Security leverages resources within federal, state, and local governments, coordinating the transition of multiple agencies and programs into a single, integrated agency focused on protecting the American people and their homeland. More than 87,000 different governmental jurisdictions at the federal, state, and local level have homeland security responsibilities. The comprehensive national strategy seeks to develop a complementary system connecting all levels of government without duplicating effort. Homeland Security is truly a "national mission." www.dhs.gov

6	OEM Ford Motor Company	Ford is the 2nd largest OEM. www.ford.com
7	Governing Body United Nations	The United Nations is the ultimate authority on standards throughout the world. www.un.org
8	Governing Body World Customs Organization	Established in 1952 as the Customs Co-operation Council, the WCO is an independent intergovernmental body whose mission is to enhance the effectiveness and efficiency of Customs administrations. With 169 Member Governments, it is the only intergovernmental worldwide organization competent in Customs matters. http://www.wcoomd.org/ie/index.html
9	Supplier LEAR	Lear Corporation is one of the world's largest suppliers of automotive interior systems and components. Lear provides complete seating systems, electronic products and electrical distribution systems. In 2006, Lear ranked #130 among the Fortune 500. Lear's world-class products are designed, engineered and manufactured by a diverse team of more than 90,000 employees at 242 facilities in 33 countries. http://www.lear.com/
10	Technology Providers i-Connect	iConnect Inc. has the worldwide presence and electronic commerce experience necessary to implement global trading communities quickly and cost effectively. http://www.iconnect-corp.com
11	Technology Providers USGCS	Global Commerce Systems, Inc. (GCS) is a consulting company that offers services designed to help commercial and government clients manage their Global Border Operations. Their solutions increase security and compliance and reduce business risks and costs helping to streamline the flow of international border traffic. http://www.usgcs.com/

Appendix B

The following questions were asked during the interview, and the interviewees were asked to document their answers and provide them to the researcher at a later time:

1) Based on your experience, what weaknesses in the global supply chain are influencing the security of your transactions?

2) What technologies have you deployed to secure of your global SC transactions?

   a. How did these technologies help you to secure the global supply chain and enhance your operational effectiveness?

3) What security measures do you use to monitor the security of your transactions in the global supply chain?

   a. Why did you select these measures?

   b. How often do you collect these measures?

   c. What do you use these measures for and how do you report them?

   d. What are the effects of these measures?

   e. How effective do you consider these measures? Why?

4) What security standards do you adopt/follow for your GSC transactions, if any? Why?

   a. How might compliance to such standards improve inventory visibility and interoperability?

   b. How has compliance impacted your security improvement efforts and IT budget?

5) What new ways or methods would you like to see implemented at a global level for the sake of improving your GSC security procedures?

---

[i] Please note that the entire conceptual solution was modeled using the Proforma® ProVision™ 5.2 Modeling Suite (AKA Case Tool). All together, there are over 20 different model types, each containing 3 or more diagrams for a total that exceeds 100 diagrams and models. For the interest of space limitations these models are not included as part of this paper, but could be made available to the interested reader upon request to the author.

[ii] Please note that the names of the individuals who were interviewed were not listed here for privacy purposes.

[iii] These 4 documents can be made available to any reader upon request of the author. For the interest of limited space, these documents are not included here.

[iv] The Questionnaire is available to any reader upon request of the author. For the interest of limited space in this paper, this Questionnaire is not included here.