

# Trustworthy Supply Chains

University of Illinois at Urbana-Champaign

Trustworthy Computing

Spring, 2006

Author: Frances Qian

## Introduction

In the starting years of 21st century, increasing competition, rising transport costs, and new opportunities with the enlargement of global trade are all playing their part in changing the global business environment. Differentiation, value creation and improved customer service are essential in maintaining our market position. Therefore, the response of supply chain and logistics from a company will be crucial nowadays.

A supply chain is the end-to-end processes, including vendors, networks and other infrastructure necessary for producing and delivering a final product or service, from the suppliers of raw materials to the end user. Supply chain management (SCM) is the process of planning, implementing, and controlling the operations of the supply chain. It goes into improving the way for a company to find the raw components it needs to produce a product or service, and to deliver the product or service to customers. SCM is the integration and management of supply chain organizations and activities through cooperative organizational relationships, effective business processes, and high levels of information sharing to create high-performing value systems that provide member organizations a sustainable competitive advantage. However, when companies become more and more reliant on technology, the growth in connectivity and any flaws of technology issues have also increased risk. To analyze and deal with these risks, we need to pay attention to supply chain operations, SCM application security, SCM investments, workforce training, corporate governance, and so on. The object is to explain some necessary key concepts and to find some possible solutions to supply chains security problems.

## Key Concepts

### Supply-Chain Risk

Today, supply chain managers are facing the challenge to recognize the full range of vulnerabilities, and then to mitigate and manage them. Vulnerabilities can only be managed if the organization has the necessary supply chain capabilities. Therefore, firms need to develop a distinctive and practical methodology to balance the supply chain vulnerabilities with the appropriate type and level of capability. They should recognize the following risks in supply chains [Handfield06].

- *Financial risk*

Supply chains vulnerabilities can result in huge financial losses and risks from excessive or mismatched inventories, and from the disrupted movement of raw material from suppliers to manufacturers [Lee05]. Companies should take on financial risk when they invest in supply chain management tools and technologies. Reducing the organization's financial risk levels is more important as supply chains become more complex.

- *Hazard risks*

Hazard risks, which involve property or casualty, refer to weather disasters, political instability, equipment shutdown, IT security breaches or product liability. This kind of risk can be man-made and natural. Insurance, mitigation plans and scenario planning are typical actions a company should take to reduce hazard risks. Building hazard-resilience communities can minimize hazard impacts and enable a company to recover from disaster faster.

- *Strategic risks*

Strategic risks relate to strategic direction and supply chain design. They are coming from technology brand collapse, disruptive competitors, stagnation, customer shift, mergers and industry consolidation, and so on. Management needs to not only understand the company's internal processes in supply chains but also monitor the external environment for relevant danger signs in order to isolate the most relevant and

critical threats. Double betting, crisis management, early warning systems, proprietary information, smart product/project sequencing, and demand innovation can be used to reduce strategic risks. The goal is to develop mitigation and contingency strategies accordingly.

- *Operation risks*

Operational risks include such major disruptions as theft, later supplier deliveries, and IT systems shutdowns. The key processes in supply chain can affect the operations of a firm's business. Alternative sourcing, backup/redundant systems and other IT approaches can improve the efficiency and reduce operation risk. It is vital to build an integrated operation risk framework that focuses on supply chains and distribution for a company.

- *Supply chain network risk*

Risks are present in a company's existing finished goods and customer fulfillment network [Scott06]. Companies should well-diversify their holdings, and have a good mix of products and a geographically-diverse inventory deployment. In this way, their risk quotient will be lower than if they make only a few products, and fulfill all demand from one central location.

### **Supply Chain Risk Events**

There have been several well-known events that disrupted supply chains. They caused intense business losses for firms because of the risks mentioned above. For example, the Taiwan earthquake of September 1999 sent shock waves through the global semiconductor market. The terrorist attack on the World Trade Center on September 11, 2001, and the August 14, 2003 blackout in the Northeastern U.S. are reminders of the potential for significant disruptions to supply chains. Disruptions from accidents in the chemical industry have led to huge economic losses and environmental damages, from the Bhopal and Exxon Valdez disasters, to the hundreds of lesser events that continue to occur on a yearly basis. Usually, if a shipment center is destroyed by a natural disaster, customers may be doing business with new suppliers. The new

suppliers might have the right to keep the business by the time the original supplier recovers from the loss and is ready to serve customers again. From shipping delays and other supply chain disruptions as reported in the Wall Street Journal during the 1990s based on matched sample comparisons, companies that experienced such disruptions under-performed their peers significantly in stock performance as well as in operating performance as reflected in costs, sales, and profits. These results add substance to the generally held intuition that supply chain disruptions should be a high priority topic for senior management and shareholders.

### **Supply Chain Network “Brittleness”**

The supply chain is a highly complex, interconnected and interdependent system. The interactions relate to several dimensions across the value chain. Therefore, it is vulnerable through the use of extended transportation, telecommunication networks and e-commerce technologies. Firms should explore the vulnerabilities and the potential consequences of terrorism and other disruptions to a global supply chain system. They should develop knowledge to model, simulate and analyze risks associated with supply chain interruption. This knowledge should be converted to decision supports, execution and management strategies, metrics and procedures. To resolve the disruption issue, framework must be designed to investigate and identify a risk factor to each link. By viewing security risks as a dimensional element of business sustainability, bottom line economic performance could be balanced with other business risks and priorities.

### **Methodology/Model/Framework**

Firms need to develop a framework for business interruption analysis. The goal is to keep the business running and lower the impact of any disruption in supply chains. One of our guest speakers, Greg Hodges from Protiviti, already pointed out: “Know risk, know reward.” The idea is all about understanding the risk so that we can figure out what additional investments need to be made to manage the supply chains, how much we are going to get out of it, what kind of risk reduction we will have, or what kind of increased revenue we shall make by increasing its compliance. According to Bovet,

there are frameworks for thinking about how to manage risk more effectively and reach the right balance with potential return that will show benefits to supply chain managers [Bovet05].

First, examine the basic supply-to-market strategy to ensure that we are following the course that best supports our business. Second, determine the right tactics to support our strategy. To execute correctly, we must have a firm grip on the firm's core strategies. In addition, we need to be willing to invest in new forms of internal analysis, such as portfolio modeling.

Bovet points out that there are two ways to do things when we think about strategy [Bovet05]: (1) Shorten the supply chain to reduce cycle time and disruption risk. (2) Optimize the portfolio of supply chain sources and locations in order to gain flexibility through diversification. The second strategy is driven from financial portfolio theory and offers a valuable framework for accessing risk/return tradeoffs. This can create a supply chain that best fits the overarching needs through a process of modeling that clearly shows managers the benefits and risks of different sourcing tactics. Firms can mix and match different tactics to maximize the supply chain's ability through portfolio modeling.

In addition, Bovet describes how the portfolio modeling works [Bovet05]:

Creating a portfolio starts with developing a set of alternative supply chain designs that support the business in different ways. For example, one design might emphasize speed to market, another might focus on manufacturing quality, and a third might home in on cost. In parallel, supply chain risks associated with each design are identified, classified, and quantified. The projected returns and risks can then be modeled and plotted on a spectrum. The optimal solution will lie along the "efficient frontier," representing the set of options with the highest return for a given level of risk. The key here is to combine supply chain elements whose disruption risks are not directly tied to each other. In other words, you are seeking to minimize the likelihood of a domino effect in which a problem at one stop in the supply chain imperils others. There may be several effective strategies to choose from, offering different combinations of risk and reward...

Portfolio modeling focuses on the business value the supply chain can deliver for a given level of risk. It is easy for CFOs and supply chain executives to understand. They can make decisions based on risks and returns. This framework is flexible enough to

adapt to any changes in supply chain in relative costs and perceived risks as well. However, Greg Hodges mentioned that current IT metrics are myopic views of volume and traffic. Metrics related to information technology have missed the mark, and they are not connected to the business. IT organizations are very project driven, not process driven. Everything is organized as if it is a one time project that will be completed, and then they move on, even after disaster recovery. Firms should consider the uncertainty related to the probability of events or future states and the exposure relates to business or process risk when they assess the risk. They should use data collection and process mapping to statistically generate scenarios of varying risk factors. This will improve the risk metrics of supply chain. Modeling tools could be explored to address the multiple objectives of reducing security risks while maintaining operational efficiencies and cost effectiveness.

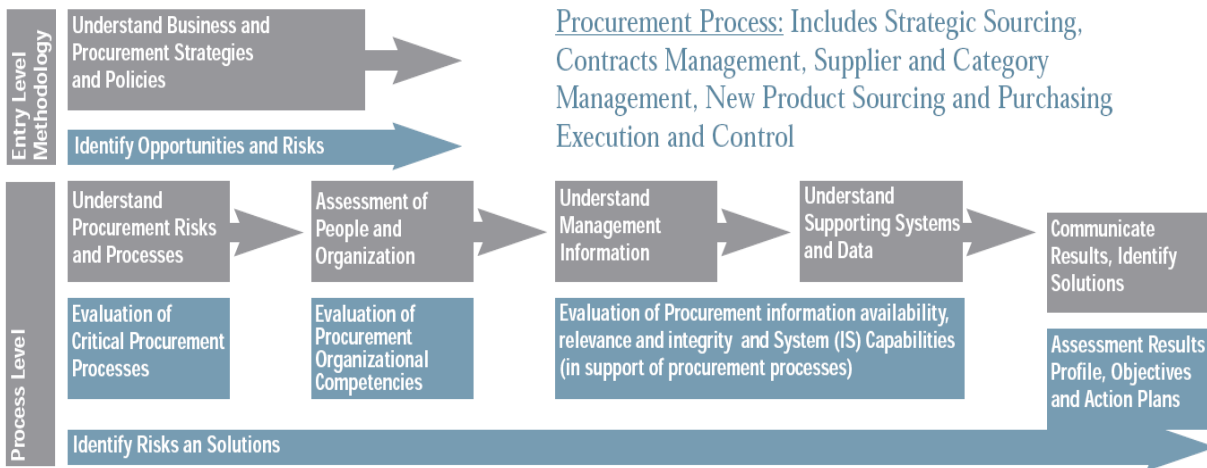
### **Sarbanes-Oxley Compliance**

There are some connections between the Sarbanes-Oxley Act and trade security initiatives [Gonzalez04]. The goal is to “protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws.” A timely, accurate and complete supply chain will help companies achieve compliance with SOA better. Corporate executives must take into consideration the complexity and risks in supply chain processes when they analyze their operations. This makes working with trading partners that share a similar commitment to security and financial integrity more important. Therefore, companies should hire a Chief Security Officer to be responsible for supply chain security, evaluate technology gaps and make appropriate investments.

### **Example**

Protiviti has produced a capabilities maturity model that assesses risks and weakness in supply chain and builds a procurement process and capabilities. This allows them to understand risks, operations and process capabilities, to assess the state, identify gaps, to benchmark leading practices, and to design and implement tactical solutions. Therefore, they are able to do efficient and effective identification, prioritize risks and mitigations, and perform improvement actions. Following is a figure of their process

[protiviti06]:



## Available Tools and Techniques:

### Extended Internet (X Internet)

The extended Internet (X Internet) is a set of technologies that connect firms' information to physical assets, products, and device [Lussanet03]. It has three basic components—networks, sensors, and services. Wireless networks carry signals to any location so that assets are remote or in motion. There are several different wireless transmission technologies, such as commercial communication satellite operators, WAN-based coverage, Wi-Fi coverage, and Bluetooth. In addition, as Dan Swartwood from Motorola mentions, ubiquitous internet protocol-based technology will be used in X Internet in the future. Sensors give assets intelligence and communication capability. They are different in type, size and price. The available sensors include GSM modems, RFID tags, and Wi-Fi tags, etc. The combination of networks and sensors enable people to serve services like tracking and tracing, monitoring, and meter reading. Research shows that executives understand key technologies but haven't adopted them [Lussanet03]. The reason is the implementation of X Internet technologies requires valuable investments, time and knowledge. The challenges include choosing the right technology combination, making decisions about the amount of budget, and selecting the right vendors, etc. Therefore, they need to know the characteristics of their supply

chain and available technologies to configure the right technologies combination.

- *Bluetooth*

Bluetooth technology is simply a short-range radio on a single chip that can translate digital data from computers. This chip can be embedded in any device. Bluetooth allows wireless communications between cell phones and other devices, among different wireless devices, between cell phones and Bluetooth-enabled appliances, and among appliances. The radio sends and receives voice and data signals generated by other Bluetooth radios that come within the broadcast range of 30 feet. Because radio waves pass through walls and other barriers, Bluetooth devices can communicate in situations that stop rival technologies, such as infrared. Thus, people do not need to be in the line-of-sight of businesses, or using line-of-sight devices, or appliances, but only within their proximity.

Bluetooth can be an important component of the architecture designed for performance of key automatic data capture technologies, which are required for today's supply chain. It can eliminate errors while gaining visibility benefits to real-time data, such as information sharing, and improved data accuracy. Wireless is a key element of both UPS and Federal Express's approaches to reduce the costs, improve their efficiency and increase their customer satisfaction rating in supply chain [Rethink04]. They replace infrared by the more flexible Bluetooth to save time. Bluetooth is deployed in their new handhelds to enable applications, such as processing credit cards. Bluetooth is also used for improving capability to facilitate time and motion.

- *Wi-Fi Networks*

Wi-Fi is short for "wireless fidelity." The name is licensed by the Wi-Fi Alliance to products that implement a set of product compatibility standards for wireless local area networks (LAN) based on the IEEE 802.11 specifications. It is widely used for mobile devices and LANs. It enables a wireless-enabled computer or personal digital assistant (PDA) to connect to the Internet when in proximity of an access point. Its data speed is about 10 Mbps and its range covers about 100 meters. Wi-Fi-enabled tags can be used to implement a tracking solution to more efficiently locate and maintain equipment. This

brings great benefits to supply chains and make a positive impact on the trucking industry. It enables constant network connections, improved coverage and faster bandwidth at affordable prices.

- RFID Tags

RFID is short for “Radio-Frequency Identification technology.” It can be used for a broad range of applications, and the focus is on the supply chain. In the future, it will play a more and more important role in supply chain management. To successfully implement and integrate the technology, enterprises will need to do upfront planning and testing. The idea of RFID is simple: Place a radio frequency transponder that contains a microchip (RFID tag) on the tracked items. The microchip will emit or reflect a signal whenever it passes under a reader. RFID tags have unique serial identifier information for a product. RFID readers can scan tags many times during a 1-second period. The serial identifier will prevent the application that makes the data request from getting multiple counts of the same items to improve the accuracy. With RFID technology, firms will know more about their inventories.

RFID seems to be an automated form of bar-code tracking. However, it is quite different because it can provide much more detailed information about the product. RFID tags have much greater capacity in storing information than bar-code labels. They can accommodate up to 96 bits of information while the Universal Product Code (UPC) labels fit only 12 to 14 bits. This could increase the visibility in the supply chain. RFID tracking also is more secure than bar coding because it is harder to tamper with. The tracking systems are intended to improve the accuracy and lower the cost of tracking goods in supply chains, warehouses and stores.

ARC Advisory group, a research firm based in Dedham, Mass, found that in 2003, the average unit price of RFID tags was 91 cents for a passive HF tag and 57 cents for a passive UHF tag. The firm expects that by 2008, the unit price will drop to an average of 16 cents for passive UHF tags. Decreasing chip prices already made RFID technology cost effective for the supply chain.

- *Wireless Handheld Devices*

Wireless innovation within the supply chain is not limited to RFID and Wi-Fi. Mobile Internet Protocol technology makes wireless handheld devices, such as mobile phones, PDAs, and laptops, also good options for firms. The wireless handheld devices offer a wide range of communications and data capture options. Companies can rely on software products to efficiently deploy, secure, monitor and maintain wireless networks and mobile devices within supply chains. Wireless often boosts efficiency and accuracy for shipments to enhance supply chains. It can support a broad range of supply management applications.

The challenge is wireless security must extend to the client by ensuring that the device is a trusted part of the network. Device keys and passwords authenticate clients and users while hiding network information. All communications need to be encrypted from end to end. For example, Halliburton's supply chain visibility is improved with wireless network for better control [Mulligan02].

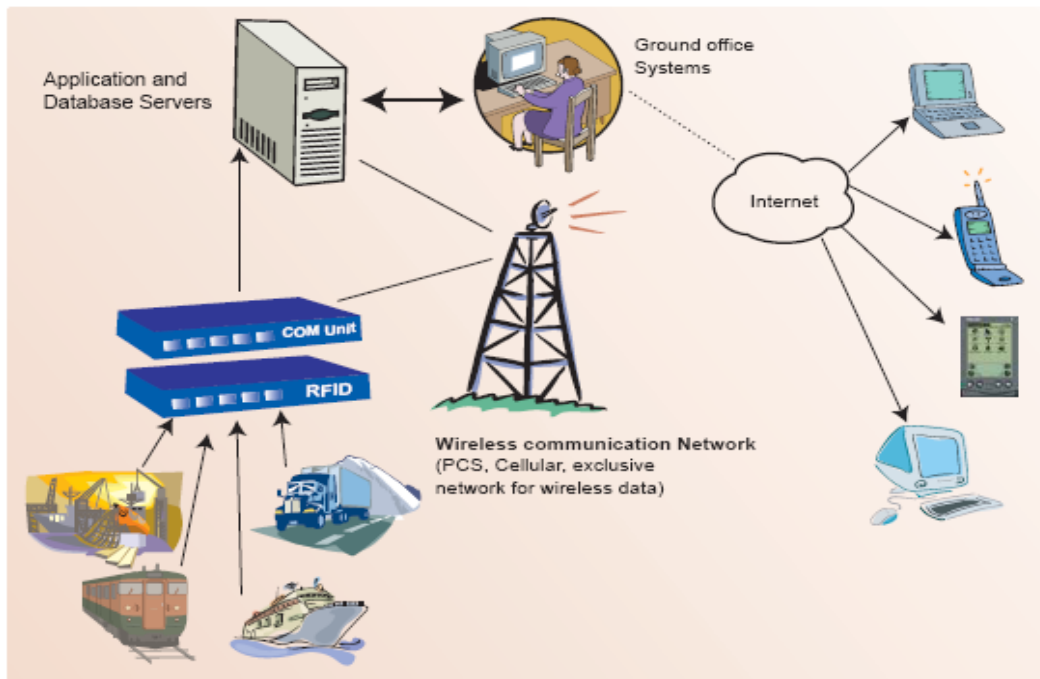
- *Wireless Tracking and Tracing*

Current tracking systems often overlook equipment and do not monitor the equipment in real time. It becomes essential for companies to reveal a significant opportunity to use wireless modes of communication for tracking and tracing the equipment now.

Global Positioning Systems (GPS) are the ideal tracking and tracing systems for global supply chains. They primarily rely on using satellites to position equipment anywhere on the globe. The data transmission can be achieved in a variety of ways, such as the mobile phone network, satellite communications for international carriers, and radio frequency systems. GPS is useful when containers are on the move. However, it offers no relief when containers are stacked in a dockyard.

A combination of RFID and GPS provides an effective and implementable tracking and tracing system that is much needed for supply chains of large companies. A GPS receiver and transmitter arrangement can be attached onto a container. The transmitter would communicate to the base station through network. Placing RFID on equipment provides accurate tracking when the containers are stacked in a dockyard. Therefore, the two technologies will become a complete tracking and tracing solution like the

following figure [Prasad02].



## Examples

Procter & Gamble Co. developed computer models to restructure their supply chain by consolidating plants by 20% and lowering supply chain costs by \$200 million a year [Anthes05]. They put their operations research group in their IT shop so that they have a crossover capability—they have as much business knowledge as they do knowledge of instruments and tools. They apply IT-assisted analytic techniques in broad areas. IT-assisted analytic technique helps them to allocate supply chain resources best. For example, simulation and optimization models allow them to mathematically try out various options, and decision analysis combines the probabilities of various outcomes and financial results for them.

RFID technology and RFID tags are more popularly adopted by companies than before. Wal-Mart uses RFID to track the flow of product from dock to stock. At the same time, Sun Microsystems, Inc already applied RFID technology to its internal manufacturing and supply chain operations. They also developed RFID technology and solutions for the pharmaceutical supply chains. The U.S. Food and Drug Administration (FDA)

reported that RFID was one of the most important tools to help improve the safety of the drug supply chains. Moreover, Sun offers other RFID solutions such as the Sun Java System Tag and Ship offering, which provides mandate compliance solution to a retailer and Department of Defense [Sun06].

Dell measures and rates its suppliers' performance on their ability to compete on cost, technology, supply predictability and service. Dell's strategy is shifting some of the inventory to its suppliers. This has reduced the risks associated with supply chain disruption, and avoided the delays and costs since the suppliers carry the risks with Dell together.

Recognizing the importance of supply chains, Motorola Inc. has already elevated the supply chain responsibility to a senior leadership level. They manage their supply chains by using vulnerability assessment, strategic planning and implementation of new processes and technologies for shipment security, perimeter security, facility access and border crossings, port security, identity management, and data integrity and sharing. Their strategy is improving relationships with their key suppliers by using better coordinated planning and forecasting as well as more frequent and detailed technology reviews. They exploit technology services and solutions as well such as RFID technology, tracking and tracing systems. Therefore, they have built an integrated supply chain to reduce risks by gaining more flexibility.

Amazon makes its supply chain applications communicate in real time by seeking technical advantages, such as RFID. Their sophisticated supply chain systems minimize human intervention, which reduces operational risks, in all the processes. Moreover, many companies have learned from incidents and disasters, such as Hurricane Katrina, Southeast Asia tsunami disaster, and Bird flu, to understand the need to have a solid supply chain with well-coordinated response. For example, the tsunami disaster placed the Sri Lankan supply chain of medicines under great strain. However, Hewlett-Packard and GE's disaster recovery plans helped them reduce the impact and the losses on their supply chains.

All these examples demonstrate how important it is for companies to make use of good risk management frameworks and modelings, and advanced technologies and tools to configure the right technologies combination, which can enhance the security of their

supply chains.

## **Relations to Other Topics**

- Risk Management
- Trustworthy Enterprises Systems
- Enterprise Information Security Policy
- Trustworthy Systems Development
- RFID
- Sarbanes-Oxley Act

## **Conclusions**

As Dan Swartwood mentioned, security is achieved by the combination of people, policy, process and technology. Therefore, we should pay more attention to the following key factors to improve the supply chain security.

### *Software Security*

As more and more advanced IT technology is used in supply chain, the security is a growing concern and remains a serious issue. The cost of not securing a supply chain could ultimately carry an even greater price. According to Grimes [Grimes04], the most cost-efficient and widely adopted wireless networking standard, the 802.11b standard, has become increasingly easy to deploy yet remains fundamentally insecure.

In addition, another European computer research founded that it is possible to insert a software virus into radio frequency identification tags, part of a microchip-based tracking technology in growing use in commercial and security applications. The commercial software developed for RFID applications potentially had the same vulnerabilities previously exploited by viruses and other malicious software, or malware, in the rest of the computer industry. A research group also warned that in a variety of situations it was possible for attackers to alter the information in an RFID tag to subvert its purpose. This added a series of worrisome prospects, including the ability of terrorists and smugglers to evade airport luggage scanning systems that will use RFID tags in the

future [Markoff06]. Thus, RFID isn't a "silver bullet" for supply chain security. In any case, with terrorists possibly on the watch for security holes in the supply chain, it isn't a good idea to put "all your eggs in one basket."

Bluetooth "is more secure than any other wireless technology" because of the short transmission range of most devices and its 128-bit encryption capabilities [Brewin04]. Still, security of wireless data remains a concern and Bluetooth transactions are not without risk. Therefore, improving encryption for Bluetooth wireless technology is quite important to lower potential security risks. Some confidential data can be obtained, anonymously and without the owner's knowledge or consent from some Bluetooth enabled mobile phones. The technology is vulnerable to the "bluesnarfing" attacks, which involves sending unsolicited text messages to other Bluetooth users, and another hacking technique called "bluejacking" [Brewin04].

In sum, companies need to recognize all the potential risks from IT issues in their systems to strengthen and assure the security of its supply chains. For supply chain security, they should design and apply processes that prevent these risks.

Knight also says that information security assures that information is protected against the exchange, loss, or introduction of erroneous information. He recommends that [Knight03]:

- Limit access to supply chain information to those with a "need to know".
- Safeguard computer access and information.
- Control access to information systems.
- Physical security in computer areas.
- Processes to backup computer system data.
- Software system should register the transactions or support operations and make a follow up of the activities that it handles.

### *Partner Cooperation and Coordination*

To greatly reduce any possible risks associated with the supply chains, it is important to call for greater cooperation and coordination among partners on the implementation of

supply chain security rules. For example, the U.S. Customs and Border Protection (CBP), who take the lead on securing borders and businesses throughout the world, launched a program that formed anti-terror partnership after the 911 terrorist attacks. Security measures were developed and adopted by this partnership. This Customers-Trade Partnership Against Terrorism is seen as the largest and most successful government-private sector partnership [Blumental06]. It has not only ensured the security of supply chains in the global trade, but also built a cooperation and trust between partners. Offering incentives to trading partners can enhance security coordination and cooperation among them.

In addition, in this ever-more connected world, business partners are taking over whole functions of each other's operations and peering into each other's computer networks. These relationships expose them to risks not only from each other, but from each other's partners. Thus, supply chain security should be extended to trading partners since it is necessary for partners in the supply chain to provide more information and support to one another to secure the system. Partners can build a good supply chain through communication, assessment, training and improvement. A partner with ineffective security could enable perpetrators to launch an attack on our supply chain systems as well as gaining access to our production schedules and pricing models, or stealing customer data and exposing a company to legal liability.

Security agreements should be written with trading partners or suppliers to strengthen the controls in supply chains. For example, Wal-Mart required its key partners and 600 of its suppliers to respond to RFID compliance mandate by adopting RFID labeling in order to continue selling to the world's largest retailer. This not only improves the security and access control in monitoring and tracking of assets, but also enables new applications such as RFID-enabled personal safety [Williams04].

### *Corporation Policy*

Deploying security standards to all employees is essential and vital for companies as insider issues continue to multiply. Configuration and policy based on security systems are a pro-active way to defend against IT security attacks. The actual standards and practices should be developed and documented or revised periodically. As Volonion

and Robinson mentioned [Volonion04], an acceptable-use policy is a security and legal necessity. The policy should be uniform for all its subsidiaries and partners to ensure security throughout the supply chain.

However, no matter how comprehensive and well written, an AUP alone is insufficient protection against misuse, abuse, and liability. Secure-use practices in the supply chain could be greatly defensive. The education, training and awareness in supply chain security should be offered to employees by companies. Implementing security policies across a range of sites and applications can be more successful by organizing and authorizing accesses.

### *Training*

As our textbook mentioned, security training still is a business afterthought. Despite tight spending, a complacent economy and the perceived commoditization of information technology (IT), 66 percent of companies in a recent survey made room in their 2003 IT budgets to dedicate more financial resources to security programs. These security programs primarily emphasized employee education, business continuity and disaster recovery. Security professionals agree that current employees still pose the biggest threat to companies' technology infrastructures, and their biggest concern is malicious attacks from viruses and unauthorized access to systems.

Security professionals can offer online courses to employees to accelerate the security training for employees and partners. The Chief of Security should often oversee the training and education seminars. As Jerry Peterson, President of Supply Chain Security, Inc. mentioned, "The ability to dramatically reduce the cost and time to deliver critical training to a large and diverse group of people involved in a company's supply chain that can affect security is critical." The company is using IntraLearn to deliver its critical security courses online to over 150 companies [IntraLearn03].

Companies should make the documentation and training budgets set at a level that is consistent with technology expenditures. The training program should point out how to recognize and react to actions on the part of others that compromise cyber security. Policies are more likely to be enforced when everyone realizes their stake in secure supply chains.

## Annotated Reference List

[Anthes05] Gray H. Anthes, *Modeling Magic: IT-based operations research builds better supply chains at Procter & Gamble*.

<http://www.computerworld.com/databasetopics/businessintelligence/story/0,10801,99484,00.html>, viewed April 10, 2006.

Notes: It describes how P&G applies IT-assisted analytic techniques in three broad areas.

[Blumental06] Dannielle Blumenthal, *Customs-Trade Partnership Against Terrorism expands security network worldwide*,

[http://www.cbp.gov/xp/CustomsToday/2006/March/ctpat\\_worldwide.xml](http://www.cbp.gov/xp/CustomsToday/2006/March/ctpat_worldwide.xml), viewed May 1, 2006.

Notes: It talks about details and benefits of the C-TPAT program developed by CBP.

[Bovet05] David Bovet, *Risk and Reward in Supply Chain Management*,

<http://hbswk.hbs.edu/item.jhtml?id=4971&t=operations>, viewed April 10, 2006.

Notes: This paper talks about strategic frameworks for managing risks for supply chain managers.

[Brewin04] Bob Brewin, *Security threats raise concerns about Bluetooth: Some IT managers take steps to limit wireless use; vendors claim risks aren't widespread*,

<http://www.computerworld.com/mobiletopics/mobile/story/0,10801,93031,00.html>, viewed April 27, 2006.

Notes: It describes Bluetooth security risks, such as bluejacking attack.

[Gonzalez04] Adrian Gonzalez, *Linking Supply Chain Security with Sarbanes-Oxley and the Bottom Line*, ARC Strategies, ARC Advisory Group, Boston, MA, August 2004.

Notes: This paper discusses the relationship between supply chain security and Sarbanes-Oxley Act, and it addresses key questions related to the impact from SOA on supply chain management.

[Handfield06] Robert B. Handfield, Jennifer Blackhurst, Christopher W. Craighead, and Debra Elkins. *A Managerial Framework for Reducing the Impact of Disruptions to the Supply Chain*, <http://scm.ncsu.edu/public/risk/risk2.html>, viewed April 9, 2006.

Notes: This article describes details about enterprise portfolio of risks, including financial risks, strategic risks, hazard risks and operational risks, and how to deal with them.

[IntraLearn03] IntraLean, *IntraLearn and Supply Chain Security Provide e-Learning to Help Fight Terrorism*, Press release.

Note: This article describes IntraLean's e-Learning software applications and courses about supply chain security.

[Knight03] Patrice Knight, *Supply Chain Security Guidelines*, International Business Machines Corporation, September 12, 2003.

Notes: This paper discusses supply chain security key elements, considerations, risk analysis, personnel control, and education and training awareness.

[Lee05] Hau Lee, *Taking the Risk Out of Supply Chains*, [http://www.gsb.stanford.edu/news/research/supplychain\\_lee\\_risk.shtml](http://www.gsb.stanford.edu/news/research/supplychain_lee_risk.shtml), viewed April 9, 2006.

Notes: This article tells us that visibility is not enough, contingency plans and tools are more important for reducing risks associated with supply chains.

[Lussanet03] Michelle de Lussanet, *Deploying X Internet Technology*, European Research Center, Forrester Research B.V., Netherlands, December 2003.

Notes: The author introduces different X Internet technologies, such as RFID tags. She shows three different case studies and points out that choosing the right technology combination is vital for companies.

[Markoff06] John Markoff, *ID tags vulnerable to software viruses, study finds*, New York Times, March 16, 2006.

Notes: This article shows that it is possible to insert a software virus into RFID.

[Mulliga02] Margaret Mulligan, *Cutting Cords Builds ERP link—wireless network improves Halliburton's supply chain visibility*, [http://epsfiles.intermec.com/eps\\_files/eps\\_cs/FS\\_Halliburton\\_cs\\_web.pdf](http://epsfiles.intermec.com/eps_files/eps_cs/FS_Halliburton_cs_web.pdf), viewed April 14, 2006.

Notes: A case study about how Halliburton Energy Services enhances its supply chains by using a wireless network and middleware.

[Prasad02] Balaji Prasad, *Wireless Track and Trace: Market Needs and Solution*, Wipro Technologies, Santa Clara, CA, 2002.

Notes: This paper introduced different existing solutions for tracking and trace systems, such as RFID technology and GPS.

[Protiviti06] Protiviti, *Supply Chain: Procurement & Supply Risk Management*.

Notes: This shows how Protiviti can help companies manage risks in supply chain by using procurement processes and capabilities.

[Rethink04] Rethink Research Associates, Gale Group, *Competition takes FedEx and UPS to the forefront of technological innovation*,

[http://www.findarticles.com/p/articles/mi\\_m0PAT/is\\_2004\\_July/ai\\_n6148566/pg\\_1](http://www.findarticles.com/p/articles/mi_m0PAT/is_2004_July/ai_n6148566/pg_1), viewed April 25, 2006.

Notes: This article talks about how FedEx and UPS used wireless technologies and tools in their systems, such as supply chain system.

[Scott06] Scott R. Sykes, *Supply Chain Risk Management—Gaining a Baseline Grasp on an Increasingly Important Challenge*,

<http://www.cscmp.org/Website/Article/Comment/Feature/Feature315.asp> , viewed April 6, 2006.

Notes: Scott shows us different risks, such as supply-side risk and demand-side risk. It also introduces supply chain network risks.

[Sun 06] *RFID in the Pharmaceutical Supply Chain*, Sun Microsystems, Inc,

[http://www.ascet.com/documents.asp?d\\_ID=3435#](http://www.ascet.com/documents.asp?d_ID=3435#), viewed May 3, 2006.

Notes: This paper introduces how Sun develops RFID technology and uses RFID tags in supply chains.

[Volonion04] Linda Volonion and Stephen R. Robinson, *Principles and Practice of Information Security*, Person, Prentice Hall, 2004.

Notes: This is a book which provides information about information security and teaches people how to make the cyber world safer and more secure.

[Williams04] David H. Williams, *The Strategic Implications of Wal-Mart's RFID Mandate*, [http://www.directionsmag.com/article.php?article\\_id=629](http://www.directionsmag.com/article.php?article_id=629), viewed May 1, 2006.

Notes: This article is about War-Mart's RFID technology, and how they use RFID in their business to enhance their supply chain systems.