June 2008

Dimensions of Supply Chain Security

James A. Pope

University of Toledo

Follow this and additional works at: https://digitalcommons.georgiasouthern.edu/sbr

Part of the Business Commons, and the Education Commons

Recommended Citation

Available at: https://digitalcommons.georgiasouthern.edu/sbr/vol33/iss2/5

This article is brought to you for free and open access by the Journals at Digital Commons@Georgia Southern. It has been accepted for inclusion in Southern Business Review by an authorized administrator of Digital Commons@Georgia Southern. For more information, please contact digitalcommons@georgiasouthern.edu.
Dimensions of Supply Chain Security

James A. Pope

In a recent column in The Wall Street Journal, executives were urged to focus on four priorities based on the events of the summer of 2007. At the top of the list was “Make supply-chain management a top priority.” The story went on to say, “Don’t wait for a crisis” (Hymowitz, 2007). Much of the story focused on supply chain security.

There has been a lot written on supply chain vulnerability during crises or disasters such as the 9-11 terrorist attack in 2001 or natural disasters such as hurricane Katrina (e.g., Melnyk et.al., 2005). Not much attention has been paid to day-to-day supply chain security. As supply chains reach around the globe, potential security concerns are present every day. The focus of this article will be on developing a framework for the topic. Given a framework, it should then be possible for organizations to develop strategies and tactics for supply chain security.

Supply chain security has four dimensions:

a. security of the product or service
b. security of the information flows
c. security of the money flows
d. security of the logistics systems

Let us look at each dimension in turn, provide a description and give examples, both good and bad.

The Product or Service

Security of the product or service itself has several dimensions. Underlying all of them is the question which the customers (meaning each successive link in the supply chain) must ask continually: “Am I getting what I ordered or expected?” Pharmaceutical companies, for example, have elaborate procedures to insure that cheap generics or even placebos are not substituted for high value drugs at some point in the distribution system (Zoellner, 2007). Their efforts are intended to insure that the end customer receives the medication that he or she is expecting. If this does not happen, lives and the company’s reputation are at risk. Pills are small, easily counterfeited and easy to conceal. The more people who handle the drug before it reaches the consumer, the greater the risk of a security breach.

A company may receive the products it ordered from a supplier, but the products may not be made to specifications. Stories of toys painted with lead based paint from China have made for sensational headlines. (Casey, 2007). Again, people’s health and lives as well as companies’ reputations are at risk from such a security breach. Ironically, the lead in the paint came largely from recycled electronic goods shipped to China from the U.S. (Fairclough, 2007).

Products may not be made to the quality standards that have been specified, or cheaper.
substitute raw materials or components may have been used. Products received may contain illegally obtained components, either through outright theft or the theft of intellectual property. You may think you have an original product, but find that you have a knock-off instead. Colgate warned consumers about authentic looking tubes of their toothpaste that were labeled “Made in South Africa” (where Colgate does not manufacture toothpaste). The toothpaste was contaminated with diethylene glycol (DEG), the same poison found in Chinese toothpaste (Colgate, 2007). Or, suppliers may simply cheat. One local businessman reported receiving a container full of rocks instead of steel from a Korean supplier.

Sometimes the length or complexity of the supply chain makes security difficult. For the agricultural product ginger, China accounts for 53.8 percent of U.S. imports. In July 2007, ginger contaminated with the pesticide aldimarb sulfoxide, a chemical which can cause adverse reactions in humans, was discovered in a California food store. The investigators uncovered seven links in the supply chain from the farmers in China to the retail store. Discovering the actual source of the contamination was virtually impossible since for any given shipment arriving in a food store, the links in the supply chain may be different each time (Zamiska, 2007).

Even in the highly regulated pharmaceutical industry problems can arise with contaminated products. Shipments of Heparin from China, made from pig intestines and used in blood thinners, were contaminated (Fairclough et al., 2008). It took months to trace the source of the contamination.

The service industry is not exempt from security issues. Many companies have found themselves in trouble with the INS because their suppliers were using undocumented workers. (160 Illegal, 2007) Or, do the subcontractors have the skills they claim to have? Countries such as Germany with a long history of guilds are stricter about the licensing of service providers than we are in the U.S. We have an array of licensing and bonding procedures to try to insure integrity (but not necessarily competence) in the service supply chain, but these vary widely from locality to locality; and, in fact, how often do we actually check these things?

In addition to these upstream issues, downstream the customer wants to feel secure that he or she is receiving the service expected. Often this may involve communication or miscommunication with no fraud involved. For example, anyone who has opened a bank account in another country knows the feeling of insecurity as to what exactly is involved. The Citizens Bank in New England (a subsidiary of the Royal Bank of Scotland) addressed this in Boston by printing their marketing materials and account information in Chinese. They wanted the large number of Chinese students in Boston universities to feel secure as customers in the supply chain (Lee, 2007).

Information

Security of the information flows is a well known problem. Since much of the information these days flows by electronic means, the data must be protected from corruption, malicious altering, or theft. Fortunately, electronic transactions are now so ubiquitous that this problem is being worked on constantly, although not always successfully. In global supply chains, there are so many issues other than security related to information flows such as timing, measurement systems, language, and so on, that security is often a relatively low priority. As a result, we hear stories of information on customers which is processed in off-shore facilities being stolen and sold to competitors. Electronic information gathering is ubiquitous (Flynn, 2007).
Information, however, is not always electronic. The Boston Globe wrapped its newspapers and those of a sister newspaper (both are owned by the New York Times Company) in paper containing the names and credit card information on 240,000 of their subscribers and left them on the streets for anyone to pick up (Gavin, 2006).

From 2006 to 2007, the theft of personal data tripled. More than 162 million records were reported lost or stolen in 2007, most in the U.S. where disclosure laws make it easier to track incidents. Arrests or prosecutions were reported in only 19 of these cases. The source of the losses ranged over schools, companies, government agencies and health organizations (Acohido, 2007).

In addition to the problem of organizations failing to protect their data adequately, a major problem is the failure of employees to take security seriously. Employees tend to value data according to the cost of the medium on which it is stored. For example, workers in the British tax agency sent (and lost) two computer disks (of nominal intrinsic value) through inter-office mail. The data on the disks had a street value of $2.5 billion. (Worthen, 2007) To make things worse, the apology letter sent to the ‘victims’ contained unnecessary confidential information. (They sent 25 million letters which means that many of them did not get to the intended recipient.) A further review showed that data had been lost from the same office eight times since 2005 (Learning, 2007).

The proliferation of laptop computers in organizations is increasing the security problems. Laptops are routinely taken out of the office (exposing them to the risk of outright theft) and connected to the home organization’s central computer through a variety of sources from home connections to wi-fi connections in hotels and airports (increasing the chances of the data being intercepted). Booz Allen Hamilton, for example, is supplying most of its 20,000 employees with laptops. Parts of the U.S. Treasury Department have up to 80 percent notebook computers in their computer mix.

Millions of laptops are lost or stolen every year; one in twenty is recovered. Eighty percent of businesses report losing one or more laptops with sensitive information on an annual basis (Charny, 2007). External threats are not the only problem. In the past ten years, the IRS has opened 4700 investigations into the illegal use of taxpayer information by its employees. The cases ranged from simple curiosity to selling the information to third parties to blackmail and extortion (Herman, 2007). IT shops are having to rethink how they maintain security of their hardware and the data contained in their machines in an environment in which it is increasingly easy to lose the data through theft or negligence.

The primary methods of electronic data protection are passwords and PINs. Both are subject to an array of problems ranging from forgetting and sharing to outright theft. A recent poll in the U.S., for example, found that the most commonly used password is ‘password.’ (10 Most Common, 2008) More advanced biometric methods such as fingerprints and retina scans have a higher degree of security, but require specialized (and relatively expensive) equipment. The most recent development which shows great promise is the methodology requiring the user to type in a string of characters (such as a sentence). This is matched with a profile the user has entered earlier. If there is a match, the user is allowed access to the system. The Psylock method developed in Germany (Bartmann, et al., 2007b) is based on thirteen different biometric parameters. It cannot be shared because the user cannot verbalize the parameters. It can even do ordinary tasks such as resetting passwords to avoid the practice of stealing passwords by falsely
requesting a new one (Bartmann et al., 2007a). In addition to its high degree of security and simplicity, the other advantages are that it requires no specialized equipment, and works anywhere there is a connection back to the central computer.

Money

Security of the money flows is often mixed in with the information flows. A prime example of this is credit cards. The use of credit cards exposes the users (both payer and payee) to the risk of the payment being diverted. Additionally, the use of credit cards exposes the payee to the risk that the personal data required to complete the transaction will be stolen and used to make purchases without the owner's knowledge, or even used to steal the owner's identity. The largest publicized case of this happening recently is the TJX security breach. Through poor security measures, TJX exposed at least 45.7 million credit card users to hackers. Their encryption protocol was weaker than that recommended for home wi-fi systems, and they retained the data too long (increasing the probability of a security breach). (Pereira, 2007)

Even if none of the data are used illegally, there is a significant cost to the banks which must reissue credit cards to their customers at a cost of around $20 per card. TJX agreed to pay Visa and its banks up to $49.5 million to cover these costs. (Banks O.K., 2007) For a relatively small investment in better security measures, management could have avoided not only the payment to Visa, but also the continuing bad publicity.

Elaborate systems have evolved to protect both the buyer and the seller in international commerce. Devices such as letters of credit were developed in an age when communication was by written document or telex and funds were transferred from bank to bank as a result of manual instructions from bank employees. In the electronic age, individuals are able to make transfers around the world from their banks to virtually any other banks. This ease of access to the system means there is a greater chance of misdirected transactions, lost transactions, or fraudulent transactions. Both the buyers and sellers must have confidence that they will receive their goods or payments if a system of international commerce is to work.

The problem of money security is becoming exacerbated as more non-traditional organizations function as banks. In parts of the developing world, for example, the mobile phone companies are performing functions, such as transferring funds, that are traditionally done by banks. At times, even, the medium of exchange is mobile phone minutes. (A Bank, 2007) As funds flow through media such as mobile phone networks instead of traditional channels, security of the money flows becomes an increasing problem.

Supply chains do not always operate within the legal system. The flow of drugs from South America to the U.S. is through a complex, well organized supply chain. To keep the flow of money back to Columbia secure, the organizations have begun using the legitimate banking system. They hire teams of workers to take bundles of cash to automatic teller machines (ATMs) in New York, making small deposits in each to avoid detection by the system. The organization in Columbia then uses the ATMs in Columbia to withdraw the funds. (Schoofs, 2007) This avoids the problem of having to carry large amounts of cash out of the U.S. (which must be reported), or engaging in complicated laundering operations. In other words, they have found a secure method of letting their money flow through the supply chain.
Logistics

Security of the logistics system is becoming ever more important. The most blatant of the problems is piracy. A ship with relief supplies for Somalia, for example, never left the port in Kenya after being warned of pirates (Ship Stays Put, 2007). A French cruise ship was seized by pirates in the same region (Pirates Seize French Ship, 2008). Piracy is common in the narrow straits between Singapore and the Philippines. Many heavily traveled shipping routes pass through areas where war or violence is common or a threat. Examples are the Strait of Hormuz or the Horn of Africa. Ninety-five percent of the world’s trade, valued at $6 trillion in 2007, travels by water. The annual plunder by pirates is estimated to be in the billions. “Ships and their crews disappear on the high seas and coastal waters every year, never to be seen again.” The problem is bad enough that the International Maritime Bureau has established a piracy reporting and rescue center in Kuala Lumpur. The U.S. Navy is active in responding to calls for help both directly and through the center (Raffaele, 2007).

Another change that is causing increasing security problems is the size of ships. Larger ships are unable or have difficulty navigating traditional shipping routes. Ships that cannot go through the Panama Canal, for example, must go around Cape Horn or the Strait of Magellan, both treacherous. Ships sailing from the west coast of the U.S. or Canada to Asia travel a great circle route near Alaska, again treacherous. Or, the East Indies, in addition to harboring pirates, have waters that are shallow and passages that are narrow. Larger ships also run the risk of losing more cargo if there is an accident. Examples are oil spills from running aground or containers falling off ships. Estimates of the number of containers that fall off ships each year range from 2000 to 10,000. An example so well known that it appeared in Ripley’s “Believe it or Not” happened in 1992 when one container full of 28,800 bathtub toys fell off a ship in the Pacific Ocean (When Cargo, 2006). Oceanographers have used the toys to track ocean currents. Some of the toys actually floated to the Atlantic Ocean.

The basic problem seems to be that shippers consider only the economies of increasingly larger ships. If they considered the trade-off between size and security, they might prefer smaller ships which are less at risk from treacherous waters because they draw less water and pirates because they are faster and more maneuverable.

Conclusion

All supply chains, internal or external, domestic or global, have four dimensions of security. As supply chains expand around the globe, and firms know less about their suppliers and have less contact with them, they, the firms, must be aware of the dimensions and devise ways of managing them. Overlooking any one of these dimensions can result in anything from a minor inconvenience to injury or death. How deeply into the supply chain one should exercise some control is a real question. The just-in-time philosophy, for example, says that we should trust our suppliers. The appropriate level of trust for a supplier in the same town or country, however, may not be appropriate for one half-way around the world. Should a firm care if its container is traveling around the Cape of Good Hope or going through the Suez Canal, as long as it...
arrives when promised?
With the framework of the dimensions of supply chain security we have presented, an organization can partition its security concerns into manageable units and organize its efforts to protect itself, its customers, and its suppliers.

References


When cargo gets lost at sea (2006). *USA Today*, 4 August.


