**Why Protect Intellectual Properties (IP)?**

Intellectual property offers an opportunity for firms to gain competitive advantage. The lesson readings highlight the benefits and risks involved in managing intellectual properties in supply chains. Intellectual properties are usually in the form of patents, copyrights, trademarks, and trade secrets. Company can issue licenses for use of their IP from which they receive royalties. In other cases, companies have sued their competitors for using their intellectual property, sometimes receiving huge compensation. Thus, protecting intellectual property affords companies the opportunity to leverage their discoveries, brand name, or trade secrets (such as information about a company process, data, designs, blueprints, formulas, ingredients, research & development activities, etc.) to gain revenue or competitive advantage. It is imperative that they protect IP especially when they engage in supply chain relationships. In supply chain exchanges, firms are expected to share information about products, demand, markets, etc. Sharing knowledge can results in mutual gains but also has risk potential. Managing knowledge in supply chain exchanges is critical especially for firms with global operations.

**Why Focus on Knowledge Management in Supply Chains?**

There are several reasons why managers need to focus on knowledge management.

1. With increased outsourcing of critical functions such as manufacturing, firms will need to share proprietary information in order to achieve the outsourcing goals. This exposes the firm to potential misuse of IP.
2. With globalization of operations, firms are engaged in business activities in different parts of the world. Some of the countries where firms operate have very weak IP protection laws. For example, there are many cases of IP loss in China, which is partly blamed on weak laws governing protection of IP.
3. Licensing relationships are typically complex and difficult to monitor. As such, licensees may act opportunistically with the knowledge that the licensor may not have ability to monitor or enforce the licensing agreement.
4. Many companies are dependent on information that is shared both internally and externally. Indeed, with increased external hosting of company information (i.e., cloud computing, software hosting, file sharing, etc.), the risk of information loss is even higher. Thus, increased flow of information between companies may raise the potential for IP loss as well as other information security breaches.
5. There is high employee mobility between companies. These employees possess tacit knowledge about their past employers and sometimes information about IP. The potential for IP leakage is therefore increased. As a result, supply chain managers need to take a keen interest in knowledge management.

**What are Challenges in Protecting Intellectual Property?**

Managers and supply chain firms encounter many challenges when protecting their IP.

1. Many companies are monetizing their IP assets through direct sales of underutilized IP assets, enforcing piracy infringement, etc. This is partly to minimize the losses of IP but also to generate new revenue streams. After all, if the IP assets have not been used in the past except illegally, then holding them may not offer much competitive edge.
2. Many companies are also adopting mechanisms to ensure that licensing relationships benefit them. However, this is not an easy task because licensing relationships are typically difficult to manage.
3. In addition, enforcement of licensing and other IP protections in many countries is inadequate. This is further compounded by increased risks of potential IP leaks as more companies engage in extensive supply chain networks.

**Summary**

* Firms need to focus on knowledge management not only because of its potential for competitive advantage but also because of the increased risk of IP loss in supply chain exchanges.
* Firms need to take cognizant of IP protection laws and enforcement when entering foreign countries. This is because the risk IP loss may be higher in these markets, which could undermine the firms’ entry to the market in the first place.
* Managers need to develop effective knowledge management measures especially in supply chain exchanges. These include the need to use relationship governance mechanisms, not just formal governance (contracts) in markets where contracts are difficult to enforce.
* Managers should explore the revenue generating potential of IP assets. Leveraging such assets can be a major source of revenue and competitiveness.

**Introduction**

Global supply chains are characterized by greater risks and security concerns. As a result, companies need to develop mechanisms to reduce risks or mitigate consequences of risk occurrence.

Increased concerns regarding the security of goods in-transit, or the disruption to supply because of terrorism, has led many companies to review their supply chains and develop contingency plans.

This lesson addresses these issues by examining various risk and security management challenges in the global supply chain.

**Risk Management (1 of 3)**

Risk is the expectation that an adverse event will occur that will be detrimental to the stakeholders in the supply chain. To understand the significance of the risk, it is important to know (1) the probability of an adverse event happening and (2) the losses associated with the event.

Risk management involves identifying the sources and nature of risk, assessing the consequences, and developing measures to avoid or mitigate risks. Managers are concerned with the probability of a risk occurring, the total effect (consequence) to the firm if the risk occurs, and what to do either to avoid or minimize the effect.

There are different sources of risk in a global supply chain. These include natural disasters (hurricanes, floods, earthquakes), epidemics (SARS, avian flu), political instability (civil war, expropriation of assets, coup d'etat), operational risks (plant breakdown, material shortage, plant accidents that cause a shutdown), terrorism and other security threats, and so forth. These acts and events cause global supply chain disruption. The first reading this week (Manuj, Dittman and Gaudenzi 2007) classifies supply chain risks into four categories: supply risk, operational risk, demand risk, and security risk.

**Risk Management (2 of 3)**

Since different sources of risk cause different levels of disruption, profiling both risks and risk prone supply chain stages is difficult. Managers need to assess vulnerabilities in the entire supply chain.

While specific risks create vulnerabilities, supply chain characteristics also contribute to vulnerability. For example, supply chains characterized by single sourcing, low buffer inventories, and/or just-in-time inventory systems tend to be more susceptible to disruption. Supply chain disruption results in increased cost, stockouts, delivery delays, congestion and increased transportation lead times, longer order cycle times, lower customer service levels, customer dissatisfaction, reduced sales, and lower performance. Consequently, managers need to develop risk mitigation strategies.

Risk mitigation involves developing approaches to prevent or minimize negative effects of supply chain disruption. Companies often develop early warning systems to detect and communicate the occurrence (or potential for occurrence) of disruption. Doing so gives the company time to address the risk. Companies might have alternative sources of supply that can be activated at a short notice, alternative modes of transportation, back-up systems, and so forth.

**Risk Management (3 of 3)**

As a mitigation strategy, companies often prepare procedures to follow if a disruption were to occur. In addition, many companies are asking their suppliers to provide contingency plans that detail alternative plans in case supply disruption occurs. Increasingly, managers are taking a proactive approach in risk management where they assess risks in supply chain processes rather than waiting to respond to risk occurrence.

Manuj, Dittman and Gaudenzi (2007) provide a comprehensive risk management process model which details five steps to improve risk management. The steps are:

1. Identifying and profiling risk
2. Risk assessment and evaluation
3. Managing risks and risk management strategies
4. SC risk management strategy implementation
5. Mitigating supply chain risks

**What are the Main Sources of Risks in Global Supply Chains?**

Supply risk – disruption in supply – supplier unreliability, price escalation, material shortages, quality issues, etc.

Operational risk – disruption in operations – machine breakdown, limited capacity, material shortages, labor conflicts, etc.

Security risk – disruption due to security breaches/ terrorism – loss of proprietary information, reduced brand equity, loss of revenue, legal liability, regulatory scrutiny, etc.

Product and process complexity – dispersion of and higher number of partners, variety of transactions, longer lead times and order cycle times, more regulations, different time zones; currency fluctuations, etc.

Increased points of contact – many parties handle shipments increasing risk of disruption.

Country of origin risks – country specific risks such as political and economic instability, etc.

Resource dependence – dependence on other firms for critical resources exposures firm to disruptive actions by partner.

Natural disasters – Disruptions due to earthquakes, volcanic eruption, hurricanes, etc.

Etc.

**Supply Chain Security**

Supply chain security refers to:

"The application of policies, procedures, and technology to protect supply chain assets (product, facilities, equipment, information, and personnel) from theft, damage, or terrorism, and to prevent the introduction of unauthorized contraband, people, or weapons of mass destruction into the supply chain."

**Types of Security Measures**

Companies protect not only their physical assets but also information and proprietary technology. Security must be multilayered, as is the case.

At a residential area, security starts with manned gates to the complex, buzzer doors at the entrance of each apartment building, and the door locks for each apartment unit. Yet, a resident will need to keep valuable items, such as jewelry and confidential documents, in a safe or in a hidden place in the apartment. Thus, although the gate is manned and the apartment is locked, the resident must at all times take measures to ensure security and prevent theft inside the apartment.

The same multi-layered approach is needed to ensure supply chain security. Companies need to ensure physical security of their facilities (background checks, access control, gates, CCTV, guards, etc.) as well as IT systems security (passwords, restricted access, anti-virus, spam filters and intrusion detectors, etc.). Companies also need to ensure the security of goods in transit (freight security) and attendant information.

**Why Should Companies Invest in Supply Chain Security? (1 of 2)**

These questions point to problems managers face when initiating and implementing global supply chain security. Supply chain security is complex given the many parties, processes, and systems that make up the chain.

Companies that invest in security can realize several benefits. Investing in security minimizes supply chain disruptions since companies are able to detect or respond to disruptions faster and more comprehensively. Disruption can lead to lost sales, the shutting down of production, and the failure to fulfill customer orders. Thus, it increases costs and impacts customer service.

Managers can borrow lessons from the total quality management. In TQM, quality defects are expensive and need to be addressed at the source. TQM emphasizes prevention and tracking of quality defects, process control, and involvement of all personnel in quality management. Similarly, supply chain security should be addressed at the source, should be monitored continuously, initiatives should involve all supply chain partners, and supply chain processes should be evaluated from time to time to detect any security gaps.

**Why Should Companies Invest in Supply Chain Security? (2 of 2)**

Since the terrorist attacks on September 11, 2001, the U.S. government has engaged the business community in developing several initiatives designed to improve the security of cargo entering the U.S. As a result, there are increased security regulations that companies must comply with. These requirements include more inspections and paperwork for goods entering the U.S. Companies that join the government-business initiatives and meet security requirements benefit from less inspection and expedited paperwork when processing their shipments.

Investing in security increases supply chain visibility because companies have a better understanding of supply chain processes and information flows. It also improves product safety by eliminating or minimizing gaps where safety could be compromised. In addition, companies improve process control by mapping the supply chain processes to identify security gaps. Other benefits of improved security include better inventory management, reduced inspections and border delays for goods coming into the country, reduced claims and insurance premiums, supply chain resiliency, higher customer satisfaction, and overall improved performance.

**Government-Business Security Initiatives (1 of 3)**

Most security initiatives adopted since September 11, 2001, often require the collaboration of the business community. In general, there has been an increase in security regulations and documentation, and inspections of goods entering the U.S. However, firms that meet certain security requirements, or who are known shippers, benefit from expedited shipments inspections at border points. As a result, companies are seeking intermediaries and third party logistics providers that clearly stipulate security procedures, and meet security compliance (including C-TPAT certification).

**Government-Business Security Initiatives (2 of 3)**

The government-business initiatives include:

* **Importer Security Filing (commonly referred to as “10+2” Rule)** - Requires importers or their agents to file “10” data elements 24 hours prior to loading of vessels destined for U.S. and the vessel operator is required to submit “2” additional data elements 48 hours after vessels departs foreign port. The main aim is to stop high-risk cargo from entering the U.S.
* **C-TPAT (Customs-Trade Partnership Against Terrorism)** - This is a voluntary program to encourage supply chain parties to improve security. Companies are required to assess their security elements and meet minimum standards published by Customs and Border Protection. Companies that join C-TPAT benefit from reduced cargo inspections, priority inspections, reduced wait times at border, etc.
* **CSI (Container Security Initiative)** - This is a bilateral agreement that places U.S. inspectors in foreign ports to inspect high risk cargo destined for the U.S. The participating foreign ports are required to implement port security procedures and automated risk management systems, and to share data with Customs and Border Protection.
* **FAST (Fast and Secure Trade)** - This is a program that allows known low-risk participants to receive expedited border crossing clearance to/from Canada and Mexico. Companies benefit from dedicated lanes, reduced inspections, etc., at the border crossings.
* **SFI (Security Freight Initiative)** - This program combines container imaging and radiation detection equipment to inspect cargo destined for the U.S. The program tests the feasibility of 100% container scanning. If implemented, the program will allow faster access to the U.S. market.

**Government-Business Security Initiatives (3 of 3)**

The benefits of implementing supply chain security initiatives include increased disruption preparedness, improved shipment tracking and supply chain visibility, reduced transit (pipeline inventory), reduced pilferage, reduced stockouts, reduced cycle times with less inspection delays at ports of entry, and improved customer service.

However, there are costs involved including the cost of changing processes to meet security requirements, security-related IT systems, redundancy (i.e., cost of maintaining excess capacity), limitations in supply chain partner choice (i.e., requirement for suppliers to meet specific security standards reduces the pool of suppliers from which a company can choose from), security compliance, increased supply chain complexity with the addition of a security management layer, etc.

**How Can Companies Improve Supply Chain Security?**

Companies can improve supply chain security in several ways. For example, Rice and Caniato (2003) discuss different approaches to improve supply chain security and resilience. (see Rice, J.B. & F. Caniato (2003), "Building a secure and resilient supply network," Supply Chain Management Review, (Sept/Oct 2003), pp. 22-30).

* Companies need to collaborate with supply chain partners in security initiatives. They need to define each company's role in ensuring a secure supply chain, and to share security goals, information on risk occurrence, contingency plans, etc.
* Managers need to realize that business and security goals sometimes conflict. For example, while a business strategy may be to work with fewer suppliers and the lowest bidder, security considerations demand working with a known shipper rather than the lowest bidder, and having alternate suppliers to reduce the risk in case the primary suppliers fail. In addition, stringent procedures to ensure security may reduce cost efficiency and responsiveness. Consequently, managers need to examine how security procedures affect the overall business strategy to align the strategies for effective and efficient operations.
* Companies need to develop flexible capabilities that allow them to respond promptly to supply chain disruptions. Initiatives include postponement strategies, multi-skilled workforce, sourcing that allows the switching of suppliers, IT systems that provide greater supply chain visibility, and contingency procedures for supply and distribution operations.
* Companies can build redundancy in their operations by maintaining a greater capacity to respond effectively to supply chain disruptions. For example, by maintaining a higher buffer inventory and excess production capacity a company can meet demand or ramp-up production in case of a supply chain disruption.
* Companies need to elevate the importance of supply chain security, and have top management buy-in. This way, they can achieve the necessary investment in security initiatives and take the measures needed to respond to a security breach.
* Companies need to acquire or invest in the IT systems necessary to enhance security. These include tracking capabilities, RFID technology, smart (tamper proof) containers, etc.
* Companies can join government-business initiatives such as the C-TPAT and FAST to ensure expedited processing of their shipments at ports of entry. This reduces transportation lead time, order cycle time, and cost.
* Companies need to adopt a security-conscious organizational culture, where every employee understands the importance of security, just as is the case with quality initiatives.
* It is important that companies develop contingency plans. Already, some companies are asking their supply chain partners to provide contingency plans as a prerequisite to signing a contract. Such measures ensure that if a disruption occurs, the supply chain will be resilient and bounce back sooner.
* Companies should use third party logistics providers that meet security requirements or are C-TPAT certified. They can also hire 3PL companies that specialize in supply chain security to help them develop secure processes and strategies.
* Companies must keep themselves informed of the changing security environment. Government security compliance requirements keep changing, and companies need to be informed of these changes. They need to have the capability to detect changes in the environment that will have significant implications on the supply chain.

**Lesson 2 Summary**

* Risk is inherent in global supply chains, and firms can’t do much to prevent most disruptions from happening.
* However, firms should be prepared to mitigate effects of SC disruptions – firms that have effective business continuity plans and other contingency measures tend to be more competitive.
* Security is a major concern in global supply chains – many firms are joining government security initiatives to ensure uninterrupted supply chain flow.
* Risk mitigation is costly – justifying such expenses is not easy. Yet, lack of preparation can have catastrophic effect.
* Risk mitigation strategies should be tailored to individual firms, business environment, and nature of risk