

White Paper

Best Practices to Deal with Threats to your Intellectual Property in the Supply Chain – by Chris Pierre, January 10, 2007

In this article we will explore five ways in which companies can help protect themselves from the theft of their intellectual property through the supply chain. These points seek to combine technology that helps track inventory through the supply chain, as well as best practices in physical security and intellectual property investigations. Specifically, the discussion will focus on the areas of inventory security, due diligence, reporting infringers, audits and investigating potential infringements.

Though many of these practices are already in use by large corporations, small and medium sized companies often find them difficult to implement with so many other demands on their budget. From a corporate culture perspective, when a company's priority is sell! sell! sell! then the protection of its products through its supply and distribution networks often gets less attention.

The ideas presented here are meant to be efficient, cost effective and scalable so that as your company's operation grows, these solutions can grow with it. Always remember to consult a lawyer on issues relating to contract law, intellectual property law, employment law, privacy and litigation to see how the ideas mentioned here can be applied to your particular situation. Now on to the ideas:

#1 Mind the Inventory: Companies typically store portable inventory in secure areas and they will hire a guarding service secure their property at night, but what about when a company's manufacturing operation is rapidly expanding and extra inventory has been brought in? The excess inventory is often left outside of the secured area simply because there isn't room inside. This material can be taken, in broad daylight.

In one example our firm dealt with, the extra inventory, which in this case was expensive and easily convertible (a term used by fraud experts to indicate that the inventory assets could be sold quickly for cash), was stored outside of the secured area and right beside the employee's locker room. Employees' knapsacks and duffle bags were lying beside the extra inventory. This was definitely a red flag.

Temporary barriers, or rented shipping containers can be used to deal with the excess inventory in the short term. It is not a perfect solution, but as a temporary measure they can be effective. The cost of these solutions will vary depending on their size and the length of time they are required for. Locking up extra inventory also sends a message that management is interested in protecting the company's physical and intellectual property.

Integrating other technologies such as Radio Frequency Identification (RFID), embedded or invisible serial numbers and other types of unique identifying technology can be very



helpful for a number of reasons. First, when investigating the origin of a product that has leaked into the black market, or when dealing with a counterfeiting case, these types of identifying technologies are invaluable. These ideas will be discussed in further detail later in this paper.

Second, RFID technology can also be used in conjunction with RFID readers and other sensors to identify when an item has left a certain geographical location. This will set off an alarm in a similar manner as when someone walks out of a retail store and the tags on the items they just purchased have not been properly scanned.

A very interesting application of this principal was developed by a company called VeriChip Corporation TM that has offices in Kanata, Ontario. They have applied RFID technology to monitor elderly people who are prone to wandering and to ensure that new born babies are not abducted from hospitals. Essentially an RFID module is attached by one of many methods to an individual, once that person travels beyond the range of the sensor, an alarm will sound and staff will come to investigate. On their website, the company states that their technologies are in use in 4000 nursing homes and in 50% of the hospitals in North America.

#2 Background Due Diligence: This is a topic I have written about often. When thinking about a new supplier arrangement, outsourcing a manufacturing function, considering a new distributor or even hiring an employee; conducting a proper background investigation is essential, and it compliments, not replaces other forms of due diligence.

Prior to entering this discussion it must be noted that these types of inquiries have to be conducted within the scope of the laws within a given jurisdiction. The local laws, combined with the resources available to gather information in that area will determine what kinds of information you are able to acquire. For example, many States in the US have an open criminal record system where for a small fee you can check county and Federal level criminal records on-line. The problem is, to be completely accurate you must conduct the inquiries in every county and state the subject has lived or conducted business in.

In Canada it is “one stop shopping.” The RCMP maintains a database of all records of criminal convictions that have not been pardoned. However, contrary to the US system described above, in order for a third party, such as an employment screening agency, an employer or an investor to do a criminal record check on an individual, that individual’s signed consent must be provided. Incidentally, authorization from the individual is required in both Canada and the United States for a third party to conduct a credit check.

Common sense suggests that when conducting background inquiries a cost/benefit analysis be conducted that considers the size of the risk being taken. By this logic you would spend more money investigating the background of a potential overseas distributor than you would of the new hire on the cleaning staff.



The logic is sound for the most part, but be advised that even low level employees may have access to your valuable inventory, or intellectual property and warrant at least a criminal record check and several reference checks for both character and employment qualifications. Many companies will offer this service for less than \$150.

The next level involves gathering information through passive, publicly available research such as reviewing a company's litigation history, records of potential bankruptcy and archived news media search. Most of this information can be accessed through the Internet, but if the databases are proprietary a subscription fee will be required to access the information.

This level of inquiry is more expensive and is generally done by investigators, librarians, research analysts or legal staff at law firms. In my experience, in North America this service can cost anywhere from a few hundred dollars to ten thousand depending on the depth of the research and how many individuals and entities are being reviewed in the inquiry.

The third level of research is more active, and more current than the other forms of research mentioned here. This level of research involves a qualified interviewer seeking out sources which may have knowledge about the company you are interested in. Sources include media experts, suppliers, former business partners, government officials customers and so on. These are people that have a strong understanding of the subject company, its executives and how they do business.

The fourth and final level of research relates to conducting due diligence in foreign countries. At the risk of stating the obvious, when dealing with foreign companies it is very important to deal with people that speak the language and know the local business landscape.

In one file I was a part of, a North American manufacturer was approached by a distributor based in Saudi Arabia. We used the information acquired by our contact in the region, plus our own research to learn that the parent company of the distributor was tied to financing Al Qaeda. In another example, the company we were researching was tied to laundering bribe money for Saddam Hussein in the Oil for Food Scandal.

When a company is considering outsourcing part of its manufacturing operations offshore, especially in a jurisdiction where litigation is difficult, it is imperative to test the integrity and controls of the offshore company. One method for doing so is to hire a local firm to purchase a product that the manufacturing company is already producing for a different client. Essentially, this is meant to determine whether or not that manufacturing company will "sell something out the back door." If they do sell the product to your buyer, then you will have your answer about the integrity of the manufacturer.



#3 Establish Methods of Reporting Fraud and Theft: According to the 2006 Report to the Nation on Occupational Fraud and Abuse published by the Association of Certified Fraud Examiners, Inc. fraud detection through tips remains the most prevalent way of detecting fraud.

In terms of a distribution of volume of tips, employees provided 64.1% of the tips identified, 18.1% came from anonymous sources, 10.7% came from customers and the remaining 7.1% were from vendors. Incidentally, for companies that are publicly traded in U.S. markets, the Sarbanes-Oxley Act requires that companies set up methods of reporting fraud. Hotlines are excellent solutions for this requirement.

Tips are just tips, and must be investigated thoroughly; however, when you have a method by which people can report intellectual property fraud against your organization, then the probability of you hearing about something bad happening is much higher.

Second, make sure that the tips can be anonymous if the tipper wishes. Of course it is most desirable to be able to interview the person that provided the information, but if all you are able to find out from them is that Company X is pirating your software, then at least you will have a starting point.

Associations or organizations may provide tipping facilities for their member companies through phone, email, or web reporting. The associations in the software industry are experts at this; they provide a hotline and a web interface to report any pirating activities of their member company's products. If you are a manufacturing organization and belong to an association, you may wish to explore what resources they have in this regard. There are also a number of third party vendors that provide this service for a fee.

In a related matter, including the discussion about unauthorized dealers selling your product is something that you should regularly bring up in sales force meetings, and in meetings with key distributors. Having open lines of communication with these two groups will help you gather intelligence on who might be violating their authorized distributor agreements, or who might be selling your product without a license, or worse, counterfeiting your product. This doesn't cost you any money at all.

#4 Security and Fraud Audits: Periodic audits can reveal when an outsourced manufacturer or distributor is breaching the terms of their contracts.

In many cases a manufacturer sells products to a network of authorized distributors. Those distributors will only be licensed to sell to end users of the products i.e. final customers, not other distributors. If that distributor is selling to known secondary market companies (or grey market companies as they are commonly known) then an audit of the licensed distributor's books may reveal that information.

Similarly if your company's outsourced manufacturer is selling your products to third parties without your permission, then they may be recording that revenue (albeit possibly

under a fictitious account name). An audit of that outsourced manufacturer may reveal some interesting information.

However, don't just stop at the financials; take a walk around the facility. Ask yourself: How easy it would be for an employee of this company to steal my product? Does it look like they are producing more here than I need for my orders? What is that third production line for? Why do they have so many employees on payroll? Why are there so many trucks in the yard? The company may know in advance that you are coming and try to hide excess inventory in transport trucks. Believe it or not, this does happen.

Your ability to conduct these audits will be determined largely by your relationship with the distributor/manufacturer and by the terms of the contract you have with them. That is the domain of legal experts and it's a good idea to speak with a lawyer in that regard.

#5 Investigate Cases Thoroughly: If you are made aware of a violation of the integrity of your supply or distribution chains, investigate them thoroughly. Again this may not be a priority for smaller companies that are interested in sales, but a leak in your supply chain can decimate your company.

This is where including RFID, various infrared, hologram or serial number technology is becoming increasingly useful. Besides the obvious benefit of inventory management, having the ability to identify a product purchased from the grey or black market as new or refurbished, distributed locally or abroad is very helpful when conducting an investigation and identifying a leak.

From an investigative standpoint, two key considerations when choosing which technology to use include the information that the identifier contains, and the difficulty in removing or reproducing the identifier. Old fashioned serial numbers printed on stickers can be removed or replaced. Serial numbers "stamped" into the sides of casings can be easily dealt with by simply replacing the casing.

Only four technologies are mentioned here but new technologies are always emerging. Digital technologies are proving more difficult for fraudsters to deal with, but rest assured, they will find a way, they always do.

All of the ideas mentioned in this report may appear to seem like common sense, but often common sense solutions are ignored. By applying security in your product life cycle, with a top down approach you can integrate process, practice, technology and intelligence in an effective manner. The goal is to protect your intellectual property, make sure that it is produced by the people it is supposed to be produced by, sold to the people it is supposed to be sold to, and that your company is rewarded for all of your research and development efforts.

Chris Pierre is a consultant with Glencastle Security Inc. an intellectual property investigation, fraud investigation and risk management consulting firm based in Ottawa, Canada. For more information please visit www.glencastlesecurity.com or contact Chris at cpierre@glencastlesecurity.com.