RISK MANAGEMENT

Coming in From the Cold: Risk Management and Economic Espionage

A definition of risk is provided in the introduction of ISO 14971, the medical device industry's definitive standard:

"It is accepted that the concept of risk has two components:
a) the probability of the occurrence of harm, that is, how often the harm may occur;
b) the consequences of that harm, that is, how severe it might be."

We know from context the "harm" discussed here is to a patient or user. However, it is interesting to note that the object of the harm is not explicit.Why does a medical device-specific standard leave out this important reference in its definition of risk? The answer, partially, is that the concept of risk itself is generic—risk attaches itself to anything we value, regardless of the specific context. In the case of medical devices, the thing that we value is health and human safety.

However, health and safety aren't the only things we value. Different forms of tangible and intangible wealth are valued by individuals as well as organizations. Where an individual might value home and family, a corporation would value product quality and employee retention. Valued assets demand protection and, based on the philosophy that "the best defense is a good offense," a risk management approach often is employed to good effect.

This bond between value and risk also is why risk management practices exist in other industries and functional specialties. Within the medical device industry, the value/risk relationship explains why risk management practices have spread from their original home in manufacturers' design and development departments, through industry standards, to all areas that affect the quality system—and beyond.

For devices, value, risk and risk management most commonly are associated with patient safety. However, this cluster of considerations can be applied equally to other types of assets. Arguably, the single most important asset class for device companies is intangible; it is the innovation and resulting intellectual property (IP)—including trade secrets—that form the basis of the industry's products and production processes.

As the world's leading producer, the US medical device industry clearly holds IP assets of enormous value, and protecting this value is an important economic risk management concern. Today, trends in outsourcing (particularly offshoring) have increased the risks associated with "economic espionage"—state-sponsored theft of valuable IP.

"I cannot think that espionage can be recommended as a technique for building an impressive civilization."
—Rebecca West

At first glance, MacDonnell "Don" Ulsch would not appear to be immersed in the shadowy world of clandestine activities. Later middle-aged, wearing khakis and a blue sports coat, he has more the look of a college professor (which he is, sometimes).

However, his resume is a laundry list of high-profile risk management assignments, including:

- Presidential advisor on counter-economic espionage strategy
- Board member (and staffer) at the National Security Institute for 13 years
- Director of Global Risk Management at PricewaterhouseCoopers
- Member of the US Secrecy Commission under former Sens. Jesse Helms (RNC) and Patrick Moynihan (D-NY)

Quoted in publications such as *The New York Times*, *Wall Street Journal*, *Business Week*, *Forbes*,*Wired* and *The Boston Globe*, Ulsch is the author of *Threat! Managing Risk in a Hostile World*, to be published later this year by the Institute of Internal Audit Research Foundation.

From his vantage point as the director of technology risk management for Jefferson Wells (a global professional services firm specializing in internal audit and risk management), Ulsch is well positioned to observe the latest trends in IP risk management. And, like any good risk management professional, he's concerned.

"Steal a little and they throw you in jail, steal a lot and they make you king."
—Bob Dylan

"The risk of IP theft has been with us for a very long time,"explained Ulsch."In fact, the first instance of America's industrial revolution—NewEngland's textile industry—was jumpstarted by IP theft." It seems that in 1811, a certain Francis Cabot Lowell (a name well known to those in New England) visited Doncaster, England. While there, he was given a tour of the local textile factory and its then state-of-the-art Cartwright Loom—the machine that had provided the British with absolute industry supremacy. While he reviewed blueprints of the loom, Lowell neglected to mention to his hosts that he had a photographic memory. In less than three years, he had put into service an exact replica of the loom and launched the US textile industry.

"The threat is more real today than it was then," said Ulsch. To illustrate, he pointed out the story of DuPont Chemist Gary Min. In November 2006, Min pleaded guilty to stealing trade secrets. A DuPont employee for 10 years, Min targeted Kevlar, Teflon, Nomex and Lucite and may have intended to sell these secrets to the government of China or Chinese businesses. As recently as this April, two Chinese nationals were arrested at the Los Angeles International Airport after attempting to smuggle sensitive electronic equipment out of the country.

For the medical device industry, the theft of IP by foreign operatives is a growing concern for two important reasons: 1) offshoring increases firms' exposure to IP theft; and 2) some countries, such as China, actively promote the theft of advanced medical technology. China conducts its economic espionage operations through its so-called "863 Program." As Ulsch explained,"Medical device manufacturers need to exercise extreme caution when transferring proprietary technology or processes to overseas partners, since foreign governments are often active sponsors of IP theft."

Ulsch also was quick to point out the moral implications of IP theft. "Government-sponsored economic espionage has created a worldwide market for stolen IP. Organized crime—even terrorist groups—target medical device and other high-tech IP because there is a ready worldwide market for it. The proceeds can be easily diverted to nefarious ends," he said. "In the US, theft of IP by organized crime has increased in particular states such as NewYork, California, Pennsylvania and Massachusetts." Coincidentally, California and Massachusetts are the largest recipients of medical device venture capital funding.

"Free competition exists inside shelters of law, custom, insurance, political approval and carefully protected status."
—Mason Cooley

So, what can a company do to manage the business and moral risk of IP theft? Ulsch advised a three-pronged approach:

- Recognize the threat is real: Many believe the threat doesn't apply to them because, "We're a small company." But the Internet contributes to a more democratic and level playing field when it comes to stealing secrets.
- Identify and valuate trade secrets: Trade secrets have value, but many companies fail to think through the revenue and value impact of loss. The value of many companies today is based largely on the inherent and future value of IP.
- Implement a definable program for safeguarding trade secrets: Evaluate threats and any regulatory requirements, and design a best practices approach that guards gainst internal as well as external threats. "Don't make the mistake of neglecting to protect secrets from employees—employees represent a significant risk of IP theft and economic espionage," Ulsch said. In case of transfers of product or process know-how, Ulsch strongly recommended tightening controls over IP. Specifically:
  - Require the right to audit on demand (and exercise this right, periodically)
  - Perform audits on either a defined or unlimited basis
  - Set supplier expectations regarding audits:
    - — Setting the "tone at top" from the onset
    - — Security officer and staff awareness training
    - — Security reporting structure
    - — Best practices, policies and procedures
    - — Employee turnover and employment incentives
  - Require disclosure of critical and material events that may elevate risk
  - Review hiring practices and background investigation processes
  - Review facility sites and assess for human-induced and natural risk, from flooding and earthquakes to automotive and aviation risk. Be particularly attentive to facilities in emerging nations that may not adhere to best practices

* * *

Obviously, effective IP risk management is a mix of high-level strategies and specialized tactics. In the final analysis, the value of medical device IP is undeniable—and, as with any valuable asset, risk and risk management are key considerations.

Marc H. Miller is president of the Crimson Life Sciences division of TransPerfect Translations. Crimson is the only translation organization in the world certified to ISO 9001:2000, ISO 13485:2003 and endorsed to ISO 14971:2000. Crimson's translation risk management processes have received official Notified Body endorsement and are patent pending. Crimson is the world's largest translation practice devoted exclusively to Class II and Class III medical devices and List A and List B IVDs. TransPerfect is the world's largest privately held, diversified language services provider with over 50 offices on 4 continents.