Word to the Wise: How to Protect Your IP from Global Threats

As strange as it seems, your company's intellectual property (IP) may be at serious risk right this minute. Yes, as you read this, it's possible that your company is under silent attack from computer hackers, spies and thieves who are trying to get at your formulas, processes, plans and research.

According to the American Association of Certified Fraud Examiners, manufacturing is third on the list of industries with the greatest number of fraud cases. Even the FBI is concerned. The organization warns that domestic and foreign rivals, start-ups and opportunists are targeting U.S. organizations in a big way.

Danger from Afar

As more companies outsource or do business overseas, the risk of IP theft has risen. Unfortunately, some of the protections we enjoy here in the U.S. are not in place overseas.

For example, you may have a non-disclosure agreement with an overseas partner, but it may not be truly enforceable. Your expectations of asset protection and safeguards may also be far beyond the reality of what's happening in rural Russia, China, India and other countries where U.S. manufacturers often outsource. It's not uncommon for outsource partners to either become or breed foreign competitors once your processes and techniques are known overseas.

In addition, according to the FBI, some foreign governments actually help their domestic corporations collect competitive intelligence, and many foreign countries don't have legal restrictions against technical surveillance.

Of course, there's plenty of danger at home as well. Cyber thieves and hackers — some acting at the behest of industry competitors — spend their days trying to get into computer networks to steal and sell proprietary assets. Some fraudsters befriend employees and offer them money to pass on trade secrets. Others will dive into your trash, take photos of your products at trade shows, or obtain your surplus equipment looking for information stored in your printers, copiers and fax machines.

What Can You Do?

Be aware of your vulnerabilities. Take simple precautions such as keeping your software security tools up to date, educating employees on email phishing and other schemes, and reminding them of security policies on a regular basis. Also keep track of all thumb drives and laptops, and don't store information that's vital to your company on any device that connects to the Internet. And be sure to quarantine suspicious email.

Also consider stealthier threats. For example, beware of on-site visitors who seek entry into restricted areas or ask questions outside the scope of their visit.

Be cautious not to disclose too much information online, in presentations and speeches, or in response to unsolicited requests for information or proposals from unknown companies. Warn employees about the possibility of outsiders showing unusual interest in their work: Their intention might be to obtain restricted data or products.

While this may sound like the stuff of spy thrillers, it's the reality of today's world. You have a lot at risk: lost revenue, loss of R&D investment and a damaged reputation, especially if your product is illegally replicated in an inferior way. Take steps now to protect the information that makes your company successful and unique.

We are committed to your success and we hope you find this information valuable. We can help you determine next steps to guard against IP theft. Contact us today to discuss your specific situation and what you need to protect.

John E. Oeltjen, CPA, CMP
Partner | Director of Manufacturing and Distribution Services
joeltjen@muellerprost.com
314.862.2070

Click here to view previous articles