

# INTELLECTUAL PROPERTY INFRINGEMENT ISSUES IN THE SEMICONDUCTOR INDUSTRY

---

JOHN CRAWFORD, DIRECTOR, BDO CONSULTING  
TOM MCLOUGHLIN, PARTNER, TECHNOLOGY PRACTICE, BDO SEIDMAN

Click fraud, identity theft, viruses and Internet security issues continue to plague consumers and curb innovation at U.S. technology companies. But as technology businesses look to expand their global reach and leverage operational processes with resellers and international business partners, they are often subjected to a more threatening security breach – intellectual property (IP) infringement.

In fact, according to the “2008 BDO Seidman RiskFactor Report for Technology Businesses,” IP infringement ranked sixth as the most common technology risk factor, reported by 84 percent of the top 100 public U.S. technology companies. To mitigate this risk, U.S. technology companies must first assess the magnitude and likelihood of threats, and then implement prevention and detection measures specific to IP fraud.

## R&D AND IP INFRINGEMENT

The semiconductor industry may be subject to a relatively greater incidence of IP infringement and IP theft than many other industries. IP may be stolen or misappropriated in many different ways. A copyrighted work may be illegally infringed by merely making and selling an unauthorized copy, as with computer software; a trademark may be infringed by selling goods identified with a counterfeit mark; a trade secret may be stolen from its owner and used to benefit a competitor; and a patent holder can be damaged by infringing activity, whether innocent or intentional.

The industry is heavily dependent on innovation or research and development (R&D) activity to produce the next technological advancement or breakthrough, which results in competitive advantage. Companies in this industry often spend up to 20 percent of their annual revenue on R&D, and the capital investments required to build new fabrication facilities can exceed 25 percent of annual revenue.

While the discoveries produced by R&D activities may be subject to confidentiality agreements, non-disclosure agreements or even patent protection, the threats which result in misappropriation are not only ever-present, but growing in magnitude as well. Secrecy is difficult to maintain in the semiconductor field because of the great mobility of scientists and engineers within the industry and their desire to publish the significant advances from R&D. The threats to secrecy which face semiconductor manufacturers include disloyal insiders, global competitors, foreign agents and even elements of organized crime.

## GLOBAL EXPANSION MAY LEAD TO GLOBAL RISK

One demographic factor that produces relatively high levels of IP infringement in the semiconductor industry is global competition. In a recent study of this issue, Semiconductor Equipment and Materials International (SEMI) identified the following countries as the areas of greatest concern to its membership: Taiwan, Mainland China, Korea and North America<sup>1</sup>. The nations which seem to generate the majority of documented IP misappropriations appear to have a strong correlation to the density of recent semiconductor industry activity (i.e., construction of fabrication plants, merger and acquisition (M&A) activity, outsourcing, partnering, etc.).

Close to 90 percent of the companies that participated in the SEMI study reported that they have experienced some form of IP violation, including infringement; counterfeiting; and theft of core technologies, core products, spare parts and components, trade secrets and trademarks. Perhaps it is not surprising that an industry which is known for rapid technological advances and the exponential rate of improvement is so susceptible to IP leakage. One plausible explanation could be the mere existence of so many valuable innovations and discoveries. Recalling famed bank robber Willie Sutton's explanation of why he robbed banks (“Because that's where the money is”), one may now know why the semiconductor industry is so exposed to IP theft.

The risk of IP theft increases as U.S. semiconductor companies expand globally and locate their production facilities in other countries. Initially, U.S. firms invested in overseas manufacturing facilities within India and China to perform the labor-intensive assembly of semiconductors for export to the United States.

However, as the technological and manufacturing capability in Asia increased, more sophisticated parts of the process have been sourced in India and China. These nations have a notoriously weak regime for IP protection, and this creates greater risk for those firms involved by making advanced technologies more readily available to those who might want to obtain them illegally.

## PREVENTION AND DETECTION MEASURES

There are numerous threats to every semiconductor business and, similarly, significant opportunities for IP theft to occur. Litigation after the fact is unlikely to restore the economic value of what is lost, and it is possible that the competitive advantages embodied by IP assets will never be restored. Accordingly, IP loss prevention is probably the best remedy, and short of that, early detection is second best.

Therefore, a proactive company management team might want to be able to answer the following questions as they pertain to some of the key management and control issues which could prevent or detect IP loss:

- Are physical security measures taken to limit access to the IP assets?
- Are access controls in place to not only limit access, but to record the identity of individuals who are provided viewing and access privileges?
- Are those who do access the IP subject to appropriate non-disclosure and confidentiality agreements?
- Are employees provided with training concerning the company's intellectual assets? Does the training include segments about the threats of economic espionage, IP theft, counterfeiting and piracy? Are such employees required to periodically acknowledge their awareness of the duty to preserve confidentiality? Are similar procedures used for third-party contractors or vendors as well?
- If IP assets are stored electronically, is access to such assets limited in nature, documented and controlled? If on a network, are there appropriate network security technologies to prevent hacking (i.e., firewalls, intrusion detection, encryption, authentication devices, etc.)? Is all access logged? Are portable storage devices prohibited from the premises?
- Are all documents clearly marked with "confidential" and "proprietary" designations? Are there written document control procedures in place to limit access and to record the true identity, date, time and purpose of individuals who are afforded access?
- Are new employees subject to pre-hire background checks? Is an exit interview conducted upon termination of employment to remind employees of their obligation not to disclose any protected information?
- Are prospective business partners and third-party affiliates subject to background checks and due diligence reviews of their business practices?
- Do IP licensing agreements contain appropriate restrictions on usage as well as non-disclosure and confidentiality provisions? Do they contain a right to surprise audits?
- Are "work for hire" provisions incorporated into employment agreements and other contracts, and are they being followed? Does the company obtain assignments of copyrighted works (i.e., blueprints or software) from consultants and independent contractors?
- Have all mask works been registered with the U.S. Patent and Trademark Office?

After these questions are answered, a risk-based review of measures, which is designed to protect the IP assets of each semiconductor company, should be conducted. Such a review might include the following steps:

- **Form a cross-functional project team.** Prior to commencing any risk review of IP assets, an effort should be made to ensure the proper team is in place. As a threshold matter, the team that conducts a review of the company's IP must have a basic understanding of the company's primary product lines, current business environment and future plans to ensure the

team remains focused primarily on the IP assets that are important to the business. The team should necessarily include at least one expert in IP law who may come from the general counsel's office.

- **Identify all IP assets held by the company.** The next step is conducting an inventory of all the semiconductor company's IP, whether patents, copyrights, trademarks, trade secrets, mask works, hardware, equipment, business methods or the like. Some IP assets are more difficult to inventory than others due to the possibility that management's responsibility may not be centralized in one area. It is necessary, however, to take a thorough and complete inventory of all IP assets, and once complete, each asset can be uniquely identified with a number, letter or symbol.
- **Ascertain the nature and scope of the rights held in each IP asset.** The company's rights could range from sole ownership to non-exclusive licenses in the IP assets. Develop a simple classification system to tag each asset (i.e., patent, trade secret, exclusive license, etc.).
- **Evaluate and value each IP asset.** Essentially, this means making a judgment about the relative strength and importance of each IP asset. For IP assets which produce licensing revenue, the value may be the annual revenues generated. For IP assets which provide competitive advantage, the value may be a barrier to market entry that is difficult to quantify. For trade secrets, perhaps there are measurable gains in production efficiency or yield that can be quantified by operations personnel.
- **Categorize and quantify risks.** For each IP asset, determine the impact to the company's operating results if the asset were impaired (i.e., misappropriated, infringed, non-infringing alternatives introduced, etc.). Perhaps a three-tiered impact rating (e.g., one (low), two (medium) and three (high)) could be employed, where asset impairment might range from a minor impact (low) to a catastrophic result (high). Then, assess the likelihood of impairment ranging from one (unlikely) to two (possible) and three (probable). The product of "impact" and "likelihood" will yield a numeric risk rating ranging from one to nine.
- **Develop a risk matrix where IP assets can be visually represented.** Such a matrix can involve a simple two-dimensional chart, with the x-axis labeled "risk rating" ranging from one to nine and the y-axis labeled "IP asset value" expressed in dollars. Each IP asset should be positioned in the matrix by its x,y coordinates (dollars by risk rating).
- **Inventory the IP asset protections in place.** For the entire portfolio, identify all management controls which have been implemented to protect the IP assets. Record or create the name of the control, develop a brief description of how the control is intended to operate, and record either the name of the individual or the management function that is responsible for the maintenance of the control.
- **Evaluate the IP asset protections in place.** Once the risk matrix has been populated with the portfolio of IP assets, it is necessary to then evaluate the degree of protection that the existing IP asset controls provide to the business. IP assets which are both extremely valuable to the semiconductor business and have a risk rating of nine should have the greatest measure of protection. A critical

review should be conducted for each IP asset, with full representation from the cross-functional team, and deliberate the degree to which the IP asset protections are adequate for risk ratings. The review should evaluate the degree to which the controls have been adequate in the past in fulfilling the intended IP management objective. It should also ensure that each IP asset protection measure includes the ability to monitor compliance and/or effectiveness in the future.

- **Develop remediation strategies.** To the extent that the evaluation reveals weaknesses or inadequacies, management should develop and implement appropriate modifications to the IP asset protections. Project management plans should be created to design and implement the necessary remediation activities. Management should also seek input from the general counsel's office regarding possible legal measures that might accompany the implementation of new or modified management controls.
- **Monitor IP asset protections.** Once the review is complete and the remediation strategies have been implemented, periodic management reports should be filed from the individual or management function that has responsibility for each IP asset protection measure. In the event that there has been a breach of control, this will afford the organization the ability to respond quickly and to mitigate any damage which may result.

## CONCLUSION

As the semiconductor industry reaps the benefits of globalization and a fertile R&D environment, management must accept that increasing expansion and innovation comes with certain risks. The risk of IP theft is real and could be devastating to a business. With a well thought out plan focused on the risks inherent to the semiconductor enterprise, a series of action points, and a monitoring and evaluation process, organizations can better identify, understand, quantify and mitigate the infringement risks facing their IP assets. ■

### *About the Authors*

*John Crawford is a director with BDO Consulting, a division of BDO Seidman, LLP, which provides litigation, investigation, restructuring and risk advisory services to a wide range of publicly traded and privately held companies. Based in Boston, Massachusetts, John can be reached at [jrcrawford@bdo.com](mailto:jrcrawford@bdo.com).*

*Tom McLoughlin is a partner in the technology practice of BDO Seidman, LLP, a national accounting firm providing assurance, tax, financial advisory and consulting services. Based in New York, New York, Tom can be reached at [tmcloughlin@bdo.com](mailto:tmcloughlin@bdo.com).*

### **Resources**

<sup>1</sup> *Innovation at Risk — Intellectual Property Challenges and Opportunities, Semiconductor Equipment and Materials International (April 2008).*