

BESIEGED

Confronting Intellectual Property Threats



CLAY SISK

by Richard Reed

Intellectual property is an organization's most important asset. It includes its knowledge, its ideas and its identity. Companies that conduct business in today's brand- and image-intensive marketplace must protect their own intellectual property and avoid infringing on the intellectual property assets of others. And with a greater reliance on technology, these exposures intensify. While it is crucial that risk managers take steps to assess and protect their organization against all intellectual property risks, three areas have emerged as hot spots: trade secrets, trademarks and privacy.

Trade Secrets

A trade secret is information of economic value that is not generally known or easily ascertainable. In an ultracompetitive environment with heightened Internet-related security and industrial espionage risks, companies must catalog trade secrets, train key employees to identify them and protect them from accidental disclosure or theft.

For example, when employees with valuable proprietary information who leave to start their own companies or to work for competitors they take that information with them. Employment contracts can help companies protect their trade secrets in these situations, but employment laws vary by state; fairly restrictive employment contracts may be acceptable in one state and unenforceable in another. Risk managers who understand their state's position can take advantage of all contractual protections available under the law in drafting nondisclosure and noncompete agreements.

Even if the state will not accept aggressive employment contracts, companies can use wage and benefit continuation as tools to protect trade secrets. A manager, at the start of his or her employment, could be asked to sign an agreement that promises a wage continuation package in exchange for protection of the company's trade secrets for a set period of time after he or she leaves.

Companies should also have effective information security policies to protect trade secrets, whether they are on paper, individual computers or a network. With inadequate protection, organizations are vulnerable to attacks that could expose strategic business plans, vendor or customer lists, or pricing information, diluting their value as business assets.

To avoid potential legal liabilities,

risk managers must be equally mindful of protecting trade secrets entrusted to them by third parties. Companies that hire employees from competitors should have policies that ensure they are not placed in a position to breach previously signed confidentiality agreements or other trade secret protections.

Trademarks

Trademark law protects an owner's use of a symbol to identify its goods and distinguish them from competing products. A key element in a trademark infringement lawsuit is the claim that the violation will create confusion in the mind of the consumer. Damages also depend on the degree of bad faith.

Litigating a trademark lawsuit can be extremely expen-



Even with strong U.S. protections, the global nature of trademark registration presents companies with significant challenges.

sive, but more important, if a company does not prevail, the goodwill associated with that brand may be lost. At the same time, trademark litigation by a large company can potentially crush a small competitor, whether or not the case has merit.

In the United States, trademark protection can derive from federal and state statutes as well as common law. The most secure protection is a mark registered with the U.S. Patent and Trademark Office. Whenever possible, companies should use a professional, commercial searching firm to establish whether other companies—particularly competitors—have already claimed rights to the same or a similar trademark.

Even with strong U.S. protections, the global nature of trademark registration presents companies with significant challenges. Companies that do business on the Internet cannot ignore this issue, even if they do not start out with global aspirations. Hav-

ing established a brand name in one country does not give a company the right to automatically use that name in another. Early in the product development life cycle, risk managers should ensure that senior management explores the new product's potential for global distribution and take steps to secure the mark in key countries.

Last year, in order to make it easier for domestic companies with overseas business to protect this intellectual property asset, the United States agreed to join an international system for managing trademarks. Under the Madrid Protocol, trademark applicants can file a single application to obtain protection in the more than sixty-five countries that have adopted the system. While the system will afford U.S. companies much broader trademark protection, it will require them to search an international register of trademarks from all of the participating countries to check if someone else owns the mark they want to use.

Once a company establishes its trademark, it must patrol its use to avoid losing legal protections. For instance, Oakley Inc., the sunglasses manufacturer, relentlessly pursues violators of its protected designs and trademarks. Working closely with law enforcement, the company's legal team oversaw the confiscation of almost 1.6 million imitation Oakley products in 2001 with an estimated street value of more than \$24 million. Oakley also vigilantly patrols the Internet, efforts that paid off when more than seventy-five hundred online auctions were shut down or cleansed of counterfeit Oakley products.

By educating law enforcement and U.S. customs officials about their companies' products, Oakley helped them more effectively identify counterfeit imports.

In addition to assiduously protecting their own intellectual property, risk managers must be equally careful in how they treat infringement claims against them. Companies should have protocols for identifying and re-

sponding to notices of potential violations. The longer it takes for a company to respond to a cease and desist letter, the higher damages may be if there is an infringement.

Privacy

Privacy rests at the intersection of technology and consumerism as perhaps the most complex intellectual property risk. Information that identifies personal preferences is juxtaposed with that person's absolute right to have personally identifiable information kept private. And the Internet has created a new realm of exposures regarding these privacy rights. But as Stephen Kobrin, a management professor at the Wharton School of the University of Pennsylvania, points out, concerns about privacy are not limited to e-commerce. It is about an age, he says, in which everything we do is recorded digitally and where companies collect vast amounts of electronic data, from medical histories to personal records and credit card transactions.

By violating the privacy of customers, even inadvertently, companies put their reputations in jeopardy with severe consequences for the bottom line. Compromising the personal information of just a few individuals can crush the confidence of a much larger group of existing and potential customers.

In addition to damaging their reputation, companies that do not take their privacy exposures seriously face the specter of regulatory enforcement and civil litigation. Fed up with direct marketing abuses and increasingly concerned about identity theft, U.S. consumers are pursuing more privacy claims in the courts. Plaintiffs have won over \$111 million in settlements or judgments against companies in 110 privacy cases against 92 corporate defendants, according to Privacy & American Business, which tracks pri-

vacuity litigation and legislation.

The U.S. government has responded to privacy concerns with legislation that targets very specific risks. The Children's Online Privacy Protection Act of 1998 prohibits operators of Web sites or online services from collecting personal information from children under 13 years of age unless there is notice and parental consent. The Health Insurance Portability and Accountability Act of 1996 prohibits the disclosure of protected health information without consent or authorization. The Gramm-Leach-Bliley Act prohibits organizations originating financial transactions from disclosing nonpublic personal information to third parties unless there is notice and disclosure permitting consumers to opt out. Other legislation deals with



By violating the privacy of customers, even inadvertently, companies put their reputations in jeopardy with severe consequences for the bottom line.

consumer fraud, telemarketing and fair credit.

While each of these laws has major implications for U.S. businesses, Congress has not passed a single, unified privacy law. State lawmakers who perceive gaps or weaknesses in federal privacy protections continue to introduce a host of privacy initiatives. Privacy & American Business expects more states to follow the lead of Minnesota, which adopted the first comprehensive Internet privacy law in May 2002. Congress is also getting pressure to mirror Europe's much stricter approach to privacy.

The transatlantic dispute over data privacy also presents a serious risk management quandary. The European Union Directive requires personal data to be "collected for specified, explicit, and legitimate purposes and not further processed in any way compatible with those purposes" without consent. The European

model—also adopted by Canada—prohibits the transfer of personal information to any country (such as the United States) that does not provide protection that the European Commission deems adequate.

Kobrin attributes the roots of the data privacy dispute between Europe and the United States to fundamental differences in cultural values—Europeans view privacy as a basic human right while in the United States, privacy is something that people can trade away for some benefit. Without an effective international agreement, Kobrin suggests, business executives must be prepared for the possibility that data flows will one day be constrained, if not cut off.

The first step in mitigating privacy risk is to understand the major causes of loss in privacy cases and to identify how those apply to their company.

There are five major causes of privacy-related losses:

1. Companies fail to recognize the growing number of regulatory requirements regarding privacy, whether imposed by federal, state or foreign regulatory bodies.

2. Companies fail to follow their stated privacy policies. Thirty-five percent of the lawsuits tracked by Privacy & American Business involved allegations that companies had disclosed consumer data in violation of their promises. Internet companies accounted for about a quarter of these cases, while 21 percent were against health care companies and 16 percent against financial services firms.

The most highly publicized case of this type involved US Bancorp, which paid \$3.5 million to settle a private class action suit and \$4 million to settle state actions. The bank had been accused of selling its customers' account information to a telemarketing firm without their permission and in violation of its privacy notices.

3. Companies fail to take adequate precautions when dealing with children and other high-risk exposures. In February, Mrs. Fields Cookies agreed to pay \$100,000 and Hershey Foods Corp. agreed to pay \$85,000 to settle

charges that their Web sites collected personal information from children without first obtaining verifiable parental consent.

4. Companies fail to link information security and privacy policies together to ensure that the information is not compromised.

5. Companies fail to dedicate resources for ongoing monitoring to ensure compliance in a fast-changing regulatory environment. According to Privacy & American Business, more than 175 important privacy bills are pending in U.S. state legislatures in early 2003.

Risk managers who underestimate the complexity of the privacy environment face a host of civil and regulatory risks. Not the least of which is the very real problem of exposing their organization to unwanted publicity that can quickly undermine one of its most valuable assets—its reputation.

What Can Risk Managers Do?


In addition to the specific actions mentioned, risk managers can take the following steps to protect their organization's intellectual property.

•*Recognize the exposures and dynamics of the industry sector.* How quickly is it changing? What are the litigation and regulatory trends in the industry and how do they impact the company?

•*Identify the risk quotient.* How much intellectual property and privacy risk can the company handle before it needs to find alternative methods of financing the risk?

•*Look for financial protection for intellectual property in different places.* Do not assume that the company does or does not have protection: check errors and omissions policies, general liability policies and directors' and of-

ficers' policies. Look for gaps in protection, and investigate specialized insurance solutions to fill them.

The combination of globalization and the Internet's continued growth has greatly increased exposure to intellectual property and privacy claims. With prudent risk management, companies can protect their prime assets, namely their identity, their trade secrets and their reputation. 

Richard Reed is vice president of Warren, New Jersey-based Chubb & Son, and global intellectual property and e-commerce practice leader for Chubb's commercial insurance business unit.

Find More:
"Getting Your IP House in Order"
RM July 2002
Archive at rmmag.com