For technology and life science firms, particularly those who use subcontractors or have high employee turnover, theft of intellectual property – patents, trademarks and copyrights* – is a real threat.

It’s a big enough problem to spark governmental action. Noting that intellectual property (IP) theft costs U.S. businesses an estimated $250 billion per year, the U.S. Commerce Secretary recently unveiled a new federal government outreach program to educate businesses on how to recognize, protect and enforce their IP rights. To learn more about your IP rights and how to enforce them, visit the United States Patent and Trademark Office Web site (www.uspto.gov) and enter “IP rights” in the search window located in the upper right hand corner of the home page.

What Can You Do?
Use these standard precautions along with sound contract management techniques to guard your intellectual property:

Precaution #1: Identify your most valuable information assets – and guard them carefully. Some technology and life science companies take too narrow a view of what constitutes intellectual property and leave valuable information without safeguards. Recent studies show that many businesses remain unprepared and uninformed about how to protect their intellectual property, such as programs, databases and source code.

Once you know what your valuables are, be careful about who you tell – and how many people have access to them. A good policy is to disclose only what’s absolutely necessary to get a job done.

Precaution #2: Register your valuables. When you produce an original work of authorship, your work is automatically and immediately under copyright. You only need to register that work with the U.S. Library of Congress Copyright Office to defend your rights regarding that work. However, you may wish to consider registering a select number of your most precious information assets (computer programs, databases, or online works) as “literary works” with the U.S. Library of Congress Copyright Office. For simple instructions on how to do this, go to: http://www.copyright.gov/register/literary.html.

Precaution #3: Use a copyright notice. Tell all viewers of your work that it’s protected if it is copyrightable. Use a copyright notice, such as ©, or the word “Copyright” and the year the work was first published. If you have a Web site, you may also want to consider posting a copyright notice on every page. Indicate who should be contacted to get approval to use any of your information. For more details on how to correctly use copyright, go to: http://www.copyright.gov.

Precaution #4: Protect your company’s rights. Make sure you have a full understanding of the acquisition of rights, licenses, releases and consents applicable to content or services contained in your work, created or provided by your company or by third parties (including work done for your company by third parties). Obtain legal review of content and services prior to dissemination.

To avoid infringing on another party’s rights, ensure that you have permission for use of others’ intellectual property that is trademarked or servicemarked. Get legal review from a Foreign Jurisdiction perspective if applicable.

Precaution #5: Consider IP insurance. IP insurance policies are now available through a limited number of specialty carriers. Costs for this coverage may vary widely. IP insurance policies provide “first party” coverage that protects your firm if you find it necessary to sue an individual or firm for stealing your intellectual property.
What is Social Engineering?
Social Engineering is a form of non-technical “hacking.” It is employed to gain important information through human interaction and involves tricking people to circumvent a normal security procedure. A social engineer may gain unauthorized access to a computer network by befriending an authorized individual and then manufacturing a bogus emergency or urgent problem that requires access to the system. By appealing to the authorized employee’s natural helpfulness and/or weaknesses, the social engineer gains the information needed to enter the system. Social engineers depend on the fact that most people don’t know the value of the information they have and, therefore, are not careful in protecting it. They search dumpsters, memorize access codes through “shoulder surfing” (looking over someone’s shoulder as they work) and successfully guessing passwords.

Protecting against social engineering requires educating your employees about the value of your information and making sure they protect it. Inform your employees about possible scams and cons used by social engineers.

It should be noted that “third party” coverage is different from the coverage described above. Third party coverage protects you and your firm if you are sued for infringing on intellectual property rights of others. Coverage for some types of IP infringement may be available through your General Liability policy. It’s important for you to review your company’s exposures and coverage with your insurance advisor so that you understand what is covered – and what isn’t.

As a professional, you need to protect your information assets as securely as possible by using these techniques. In addition, diligent contract management can help guard your company’s valuable intellectual property from misuse and theft.

Contract Protection
Effective contract management with subcontractors, employees and clients can also help protect your company against IP theft.

Although contracts will differ based on the circumstances of each situation, you should always make sure you fully understand any agreement before signing on the dotted line. The contract should clearly communicate each party’s expectations to avoid misunderstandings down the road. Legal review of any contract is an advisable practice. Ensuring that all contract paperwork is in order is just as important to successfully managing your business and company assets as closing the deal.

Employee Contracts
Most IP thefts are committed by individuals you know and trust – your employees, temps, subcontractors, consultants and janitors. In fact, experts agree that the people who work for you pose the greatest threats.

The explosion of multiple electronic channels of communication in recent years – e-mail, instant messaging, Web mail, blogs, chat rooms and handhelds – present an increasing threat to IP security, according to a recent survey of financial services firm employees by Orchestria. More than 75 percent of the employees surveyed felt that it would be easy to send proprietary information outside of the company.

In some cases, they can steal confidential information from you during their term of employment and then use it at competing firms when they go to work for them. In other cases, employees or former employees may unwittingly divulge confidential information. Unscrupulous individuals may employ social engineering to cleverly manipulate your employees into giving away information that will help them to gain unauthorized access to your system and the information that resides there.

The survey points out that most breaches of IP policy are due to a misunderstanding of company policy, rather than malicious acts. This fact highlights the need for businesses to make sure they have a clear policy on employee disclosure of IP and to ensure that electronic communications are monitored and controlled effectively.

So how can a business grow and add staff, yet protect itself at the same time? Asking employees to sign an employment contract with your firm is a good place to start. Employment contracts should include both non-disclosure clauses – which prohibit employees from releasing confidential or proprietary information and non-compete clauses – which limit employees’ ability to work for a competitor or set up a competing business. It is also important to implement a control system,
including signed agreements, for your company’s employees, new hires and subcontractors that ensures that these parties do not share, divulge, disseminate or use a previous employer’s or client’s trade secrets or other intellectual property in their work for you.

When employees resign from your firm, conduct exit interviews to remind them of the terms they agreed to when they started. In the event of a lawsuit, thorough pre- and post-employment steps can prove you took precautions to safeguard sensitive information.

Contracts with Subcontractors
To protect your interests when outsourcing work to subcontractors, ask each contractor to sign an agreement at the start of a project. Spell out your expectations for confidentiality, ownership of code, program or notes they produce so there’s no confusion.

Here are some other tips on how to effectively manage these contracts to guard against the virtually invisible threat of IP theft:

- **Have an attorney review and prepare all legal contracts.** He or she can make sure you have the protection you need.

- **Make sure all parties, as well as their roles and responsibilities are identified in your contract.** Don’t make assumptions or rely on a conversation or e-mail for details. As a general rule, if it’s not included in the contract, it’s not part of the deal.

- **Be specific about the scope of the project, deliverables, when they’re due, and for how long your particular contract is in effect.** Don’t allow “scope creep” to occur. If a client makes changes that require additional work, write up another contract for the extra project including the revised expectations, time frames and costs.

- **Make sure the contract is enforceable in your state.** Don’t assume that because you put something in your contract, it will hold up in court. For example, not all states treat the enforceability of an indemnification provision the same.

- **Spell out venue, choice of law and jurisdiction, particularly if the subcontractor you’re working with is located out of the country.** Specify a choice of law that is favorable to you, or, at the very least, one that you and your subcontractor can both agree upon. Don’t assume that U.S. laws will govern your contract if you do business with foreign subcontractors.

### Client Contracts
Thorough contract management also requires vigilance when signing contracts with new clients.

No matter how excited you may be about winning a bid, don’t throw common sense out the window. It’s important to understand the terms of the contract: what you’re being asked to do, how fast you’ll be expected to complete it, the payment terms, the implications for breaching the contract, and whether there are any stipulations that you carry specified types of insurance coverage or limits.

A growing trend is the practice of shifting liability to another party if something – anything – goes wrong. Make sure that the contract doesn’t saddle your company with all liability. Legal review is an essential and worthwhile expense.

The following clauses should raise a red flag if they appear in a contract you’re asked to sign.

<table>
<thead>
<tr>
<th>Clause in Your Contract …</th>
<th>Could Mean That You Agree to …</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Right to Sue Waiver</strong></td>
<td>Give up the right to sue if something goes wrong with a project.</td>
</tr>
<tr>
<td><strong>Consequential Damages</strong></td>
<td>Accept responsibility for losses that may not be the direct result of your software, code or service.</td>
</tr>
<tr>
<td><strong>Penalty Provision</strong></td>
<td>Be responsible for predetermined penalties and costs above and beyond the direct damages if a problem arises.</td>
</tr>
<tr>
<td><strong>Indemnity clause</strong></td>
<td>Accept the burden of responsibility for a loss – even though it may not be entirely your fault.</td>
</tr>
</tbody>
</table>

What if you really want to accept a project, but don’t like the terms of the deal? You should always try to negotiate the terms that are most problematic. In some cases, you may be better off turning down a project than accepting the terms of the contract.
If so, do a cost-benefit analysis which itemizes all the pros and cons to ultimately decide if the project is right for your firm. Can you truly afford the financial risks associated with fulfilling the contract? Sometimes, the right choice may be to say “no” to the job.

Protecting your business against intellectual property theft is essential in today’s business environment. It’s important that you know how to recognize, protect and enforce your IP rights.

Trademarks, Copyrights, Patents – What’s the Difference?

A trademark is a word, name, phrase, symbol or design – or any combination of these – that identifies and distinguishes a specific product from others. For trademark information, go to www.uspto.gov/main/trademarks.htm.

A copyright protects an original artistic, literary, dramatic or musical work presented as a book, photograph, movie or other tangible medium. For copyright information, go to www.copyright.gov.

A patent protects an invention, which includes a process or a machine. Receiving a patent for an invention means that others are excluded from making, using or selling the invention. For patent information, go to www.uspto.gov/main/patents.htm.

For More Information

For more information on how to manage risks for your business, contact your local Hartford agent, or visit www.thehartford.com.

Best Practices for Your Business

About The Hartford’s Technology Practice Group

For more than 25 years, The Hartford has insured technology and life science businesses of all sizes. Our products are flexible enough to grow with a business – from a startup or sole proprietorship to a large, publicly traded company. We also offer services that can help businesses lower their losses, like our series of Technology Best Practices.

* This Best Practices focuses primarily on copyright. For additional information on patents and trademarks, please consult your attorney or legal advisor.

The Best Practice provided in these materials is intended to be general and advisory in nature. It shall not be considered legal advice. The Hartford does not warrant that the implementation of any view or recommendation contained herein will: (i) result in the elimination of any unsafe conditions at your business locations or with respect to your business operations; or (ii) will be an appropriate legal or business practice. The Hartford assumes no responsibility for the control or correction of hazards or legal compliance with respect to your practices, and the views and recommendations contained herein shall not constitute or undertaking, on your behalf or for the benefits of others, to determine or warrant that your business premises, locations or operations are safe or healthful, or are in compliance with any law, rule or regulation. Readers seeking to resolve specific safety, legal or business issues or concerns related to the information provided in these materials should consult their safety consultant, attorney or business advisors. All information and representations herein are as of January 2010.