Protect Your Intellectual Property!

Theft of confidential information and trade secrets can be just as damaging to your business as embezzlement. Information theft is a serious issue. Your intellectual property is one of the most important assets of your business. In the hands of others, your business may suffer greatly.

Case #1: David Olsen bought a sheet metal fabrication company and over many years put every nickel of his money and every ounce of his energy into making it a success. Over a long time he courted and finally secured a large convenience store company as a customer. He did so by designing a new fuel pump canopy that the store decided to adopt. It was a great account with the promise of many years of profitable business. But an employee–unaware of the proprietary nature of the designs and drawings–provided a copy to the purchasing agent of the customer. It was not long before the customer had found someone to make the canopy for a lot less money.

Case #2: Tom Wirt was a likeable person, a natural salesman quick to establish relationships. He became a valuable rainmaker for Bolder Engineering and made a very nice living. He began using company connections to forge personal business deals "on the side." The owner tolerated it and it became, no doubt, a valuable perquisite of the job. But there was no stopping Tom's climb. The day came when he resigned and started his own firm. He took a significant amount of Bolder's business with him. It's been six years and Bill Bolder will tell you–he would have been far better off if he'd never hired Tom Wirt.

What could David Olsen have done? Protect his valuable asset. How? By educating his employees on the confidentiality of the company's intellectual property. By restricting employee access to drawings. By copyrighting each set of drawings and prohibiting copying of them. By closely tracking each set.

What could Bill Bolder have done? Require Tom Wirt to sign and maintain a strict but enforceable non-compete agreement. And possibly either letting Wirt go before his ability to damage Bolder rose to unacceptable levels and/or working out a long-term deal with Wirt that would prevent him from leaving. The main thing is, address the issue and take precautions before it is too late.

What about your company? Your intellectual property? Maybe you should take an inventory of your vulnerabilities and begin managing them properly. Here are some suggestions.

1. *List and describe your intellectual property.* Ask yourself and your employees what information you have that is proprietary, sensitive and confidential? Who might have an interest in these data? If these data were to "get out," what kinds of things could happen? How might this harm you, your customers or your vendors?

2. *Use computer passwords.* Require your employees to use passwords to access your computers or network. This will serve to keep unauthorized people away from important files. Don't let employees get lazy with their passwords–require they be changed monthly. Dissuade people from using features that "remember" passwords. This can make it easy for an unauthorized person to gain access to your system. Insist that users log off your network

whenever they're away from their desks, so unauthorized users can't jump in from their workstations.

3. *Have all employees sign non-disclosure agreements*. Make sure employees understand that theft of intellectual property is as serious to your business as theft of physical property. Use a non-disclosure agreement or a non-disclosure clause in an employment contract to spell out employees' responsibilities for confidential or trade secret information. Be sure you define what your company considers confidential. This is critical, because it clearly differentiates which information belongs to your company and which belongs to the employee. The agreement also should outline steps the employee must take to maintain confidentiality, such as using computer passwords, not removing sales lists from the premises, not copying documents to disk, etc.

4. *Keep tabs on your documents.* Set and enforce strict procedures for access to trade secret and confidential or proprietary information. Create a hierarchy of access among your employees for sensitive information. Allow only those who need certain information to see it. For example, a sales rep may need customer contact information for his or her territory. But the rep does not need your entire client list, and does not need access to billing data. Label key electronic documents (such as your customer database) as "read only" so they cannot be altered or written to disk.

5. *Don't tempt prying eyes.* Don't make it easy for people who aren't supposed to see confidential documents to snoop. Encourage everyone at your business to take certain basic precautions. Never leave documents lying around. File things away when you're done with them or when you're away from your desk. Lock your filing cabinet and your desk when you're away. Close computer files when they are not being used and never leave a file on your screen when you go away from your desk.

6. *Have a plan for terminated employees.* Don't let a disgruntled ex-employee become a security threat. Have a plan in place to keep a person from leaving your company with confidential documents. Some steps to follow include:

a. Have the person leave the company immediately upon termination. Letting an employee hang around a few days to get his or her affairs in order only invites this person to make off with papers and other information that might be valuable to your firm. Have a supervisor stand by while the employee removes personal possessions from his or her desk.

b. Make arrangement for immediate return of any confidential company information such as client lists, price lists, etc. Make the timely return of these documents a condition of receiving severance pay.

c. Insist that the person turn in keys both for the business premises and his or her desk and file cabinet. If he or she doesn't return them, change your locks.

d. Immediately sever the person's access to your computer network. This is especially important if the person can dial in to your network from home, and then simply log in and download important information.

7. *Buy cross-cut paper shredders–and use them.* Be careful when you are throwing out copies of sensitive or confidential documents. These include financial statements, proposals, customer information, reports, receipts, bills, invoices, etc. Don’t just toss these in the trash. Shred them. Putting them in the garbage unshredded opens up a range of security issues. If your trash is not disposed of properly, these documents could easily end up in the wrong hands–or blowing down the street past prying eyes. Are you serious about your business and long-term growth? Protect it from harm. Protect its intellectual property.