

Protecting Your Secrets

The World War II saying of “loose lips sink ships” is even more relevant in today’s fast-paced environment and the world of electronic communication. What seems to us as ordinary information can be extremely beneficial to our competitors. If public power entities are to keep their edge over their private counterparts in this increasingly competitive environment, keeping the company’s operational secrets confidential is now more important than ever. Generally speaking, information can’t be protected legally as a trade secret if it has ever been, even temporarily,

- Put on the Internet
- Exhibited at a trade or marketing show
- Explained to a customer over the phone
- Discussed in a speech; or
- Otherwise revealed without a specific confidentiality restriction

Thus, it is important to remember that even routine and seemingly insignificant information may be valuable to other companies, and as such, the first line of defense is to first determine what information you have that the competitor does not have and whether that information adds value or provides an advantage to your company.

General Thoughts

Just about any information which reveals how your company performs its daily business can be useful to a competitor and damage your company’s position in the energy market. However, the “crown jewel” information must belong exclusively to your company because what is often overlooked is how the information was acquired and how it was developed to determine if it was already available to the public or known to others in the industry. While a company must be able to accomplish its business goals, confidential information is a form of property and a company must condition access to it, or even employment itself upon an agreement not to use it or disclose it. The extent of protection will vary depending on the circumstances under which the information is exchanged and the tangible form of the information. Some general guidelines concerning confidential information are:

- All information with which you are entrusted should be assumed to be confidential unless you are advised to the contrary; and
- If you ever have to ask whether to keep something confidential, trust your gut feeling and don’t disclose the information.

The greatest risk of losing the “crown jewels” comes from the loss of secrecy. The greatest source of this risk may come from new hires, and consultants who have access to the information and don’t recognize the importance of the information. People are the weakest link in any confidentiality system, and the headlines are full of numerous instances of inadvertent and deliberate disclosures. Closer to home are the slow-drip disclosures of business plans, customer opportunities and product-offering roadmaps that can result in the loss of a competitive advantage. The problem occurs every day as employees chat on the phone at restaurants, bars or gyms and someone overhears. Those that hear will definitely capitalize on every opportunity to beat the competition by using this information to their advantage or in selling their services to competitors of your company.

Maintaining Confidentiality

A company should begin by classifying all information that you possess into categories of confidential information. These categories are:

- Public: can be freely disclosed in marketing materials
- Confidential: information like product specifications that can be disclosed if the recipient has signed a non-disclosure agreement
- Company-confidential: information that should not be disclosed to any outsiders even if they sign non-disclosure agreements such as supplier lists, pricing information; individual customer terms and conditions, and source code; and
- Project-confidential: information that should not be disclosed outside the particular project or project team.

Once this is accomplished, the information can be given, received and exchanged in the following ways:

- Through the Public Relations Department for external distribution of general and specific information relevant to your operations;
- For internal distribution, as conveyed with the following statement :
"The attached document contains privileged and/or competitively sensitive information. It is provided to you with the understanding that its contents are to be used only to the extent necessary for _____ company's internal purposes, and its contents are to be shared on an internal need-to-know basis only. Please maintain this information in a secure, restricted-access location, and establish controls in your office to provide that access is only gained through your personal approval."
- When working on projects with co-workers, identify all key personnel who will or should have access to the information. Limit the number of people who have a "need to know".
- Determine what materials should be confidential before their creation and subsequent distribution. It will be impossible to retract information after it has been distributed.
- Mark all materials as "confidential." Doing so alerts others that the contents are confidential and should not be distributed or copied.
- Limit the number of copies and the people to whom the information will be distributed. If the information has to be widely distributed for comment, notify the recipients that the information is considered competitively sensitive and request that the document be returned to you and not copied.

Stopping Loose Lips

Maintaining the confidentiality of information while dealing with customers, vendors, and consultants is extremely important; however, the process of keeping information confidential starts first at home with keeping employees in line. The process needs to start before people are hired, especially in situations where the person has worked in a similar position for a competitor and there is an opportunity for the inadvertent or deliberate use of confidential information from the competitor that could land your company in hot water. If such a person is hired, he or she should be counseled to not use any information from his or her previous position and that discussion should be documented so as to insulate your company against liability if the employee ignores your instructions.

When a new employee is hired, his or her employment should be conditional on the employee signing a confidentiality agreement requiring the employee keeping all the company's confidential and competitively sensitive information confidential. This agreement should be explained fully to the new hire so that the employee understands what will be expected of him or her. Additionally, the employee should receive regular training on this subject, which can take the form of large lectures or individualized on-line training. If the employee participates on projects, the project kick-off meeting should include a reminder that

the project-specific confidential information must be used only within the project and cannot be used on other company projects or discussed with other non-project employees. This reminder should later be memorialized in the meeting's minutes. And lastly, before your employees attend trade shows and conferences, they should be reminded at a pre-meeting not to mention or discuss company business or make cell calls about company business in open spaces like a plane or in an elevator, or at a coffee break, on the trade floor, or at surrounding cafes or restaurants.

When an employee leaves the company, the exit interview should include a reminder to the employee about his or her continuing confidentiality obligations. The employee should also sign an agreement confirming that he or she has returned all copies of the company's confidential information.

Keeping Tabs on Others

It is often necessary to allow contractors or consultants access to confidential data, and you need to ensure that they first have effective systems and processes in place to protect the information. The eventual agreement to engage the contractor or consultant should require the party to use the same level of care it uses to protect its own confidential information (but no less than reasonable care) in order to keep all of your company's confidential information confidential. The agreement should also impose similar confidentiality provisions on all employees of the contractors or consultants and state the severe consequences associated with breach of the confidentiality obligations, such as termination of the project or collection of a significant amount of damages. Vigilance in protecting the crown jewels must be also used as contractor or consultant contracts are renewed or revised. Changes to the scope of the consultant's duties may change the scope of the information, or the authority or anticipated use of the information by the consultant.

A company should not disclose particularly sensitive information to customers, suppliers or commercial partners, but rather a subset of the information that is not "company-confidential" or "project-confidential". All information that is disclosed must bear the mark "Confidential and Proprietary to _____ Company", and the use of watermarks embedded in the document is also useful to make the information recognizable as your company's proprietary information. However, understand when you do disclose, you are giving away information that did not come easily or inexpensively to your company, and it is usually not yours to give in most instances. This is not to say that you should not be cooperative with others or attempt to strike a deal with an interested party. Rather, be aware that disclosure should be confined to what is essential for you to do your job in a professional manner.

If you are disclosing particularly sensitive information to another person or company, you should also try to track the information through the recipient party. If for some reason, the crown jewels are misappropriated or misused by others, the likelihood and expense of litigation in pursuing the person who does this is largely dependent on what steps your company took to protect the information before the alleged misappropriation occurred. One suggestion is to periodically check the other party's website, if applicable, and search for the use of your proprietary information in their marketing and business information. If a disclosure has occurred, an immediate response from you to the breaching party should be forthcoming such as a cease-and-desist letter or filing for injunctive relief.

Physical Security

In order to properly safeguard confidential information, physical security is of utmost importance. Physical security is only as strong as the individuals using it, and the temptation is ever present to be lax in this regard. The greatest source of security breaches comes from the acts of customer service personnel who, in their effort to be seen as helpful and service-oriented, provide access to others without clear authority. Your company's place of housing such information should be locked and accessed only through a restricted password, identity card or key. If a password is used, the password should be changed regularly. If a project includes project-confidential information, the information should be kept in a separate

section of the premises with access restricted to the project members. If an access card is used, the card should identify the person in sufficient detail but not contain any company-specific information so that if it is left on a bus or at a meeting off-site, the person finding the card will have no idea where to use it. Information that will be sent via fax or copier should be sent to a fax or copier that is not in a shared work area. In the case of project-confidential information, the project should have a dedicated fax machine in the project area for this purpose. If this is not possible, members of the team should be advised to collect their documents quickly rather than to leave them sitting unattended on the machine.

Your company should shred all unnecessary copies of confidential information subject to your company's retention policy. The location of the shredder should be part of the information provided to new hires and as an ongoing reminder to all employees. Filing cabinets should be locked and all whiteboards cleaned at the end of meetings. In the case of a project, the project should have a specific meeting room and portable whiteboard.

All desktop computers and laptops, mobile phones, PDAs and Blackberrys® should have passwords for identifying authorized users and if these machines are left unattended for a short period of time, the screen should go dark and lock. Thought should also be given to forbidding the use of such devices by certain customer care and contact employees to minimize the possibility of these individuals downloading company-confidential information. Similarly, information can be transmitted by e-mail or zip drive outside the company in a matter of seconds. If there are concerns about what you are saying, or the content of information is particularly sensitive, try using the old-fashioned method of placing a phone call rather than e-mailing it and making it available to potentially thousands on the same server, or make a hard copy of the report and hand-deliver it to the intended recipient. Lastly, before any computers are scrapped, their hard drives should be thoroughly erased or physically destroyed.

Conclusion

As public utilities enter into an age of electric deregulation and competition, the issue of keeping trade secrets safe becomes increasingly important. In accordance with Texas Senate Bill 7, passed in 1999, CPS Energy has by resolution adopted an extensive list of competitively sensitive and confidential information that need not be disclosed to the public. This resolution gives CPS Energy increased control over the distribution of confidential information that may not have been previously protected by law and gives CPS Energy similar ability to control the dissemination of information that private utilities have previously enjoyed. Only in this manner and in employing the mechanisms discussed in this paper can a public utility continue to widen its advantage to be successful in the fast-approaching competitive utility energy market.

Concerns about national security intensify during wartime. With German and Japanese submarines patrolling off U.S. coasts, great emphasis was placed on educating servicemen and civilians about the need for secrecy concerning military matters, especially troop movements. Central to maintaining national security was the Office of War Information's drive to limit talk about the war in both the public and private arenas of American life. Silence meant security. The graphic designs of this "loose talk" on the home front posters were usually strong and eye catching using bright colors for impact. In no other series of WWII posters was the potential for loss of human life portrayed as such a recurring theme.

Two trade secret stories received considerable media attention recently. One featured Apple Computer's decision to drop an appeal in a case involving two online journalists who published company secrets. The other reported federal indictment of a former Coca-Cola secretary and associates who offered to sell secrets to Pepsi.

Neither involved a whistle-blower's exposing corporate misbehavior. Nothing suggests differences in the value of the information. Rather, both cases apparently relate to harm associated with premature notice of new products.

Yet, people who published what they knew to be Apple's secrets have been praised for refusing to reveal sources, whereas Pepsi employees have been praised for refusing an offer to buy secrets. Moreover, after the FBI intervened in the latter case, the Coke secretary and associates were indicted.

An AP reporter observed in the context of one case that: "Stealing trade secrets is not uncommon in a competitive corporate culture where heavy premiums are placed on [being first in the market. In late October, although the former Coca-Cola secretary was still scheduled to stand trial, the two men who helped each pled guilty to conspiracy. For merely offering to sell what they understood to be a valuable secret, they face up to 10 years in prison and \$250,000 in fines.

The case of *Weigh Systems South v. Mark's Scales & Equipment* involved two former Weigh employees—a manager who started a competing firm, Mark's Scales & Equipment, and a service technician who joined him at the new company. Weigh alleged that its former employees stole proprietary information on their way out the door.

Weigh filed a complaint seeking damages and injunctive relief, alleging that the former employees and Mark's Scales violated the Arkansas Trade Secrets Act. Weigh asserted that its former employees had misappropriated its customer and vendor lists, pricing information, software, service agreement inventory checklist and marketing plans—all of which constituted trade secrets.
