Information Loss:
Reducing Your Biggest Risk

By Naomi Fine

EARTHQUAKE, FIRE, FLOOD, RIOTS AND A TELEPHONE CALL. Each of these can be catastrophic to a company. A telephone conversation that reveals a company's secrets to a competitor, can be more damaging to a company than any natural disaster or civil insurrection. One company discovered this when they set out to develop a business contingency plan. As they discussed all of the potential disasters that might befall the company, it became clear that the loss of intellectual property, whether by intentional or accidental means, was the greatest risk the company faced.

Confidential information is every company's lifeblood because it is comprised of the strategies and tactics that bring the company success. A company's proprietary information is what differentiates it from other companies in the marketplace. The good news is that a company's highly valuable information is not likely to be lost in the event of an earthquake, fire, flood or riot. The bad news is that confidential information can be lost in the course of an innocent telephone discussion.

BALANCING INTERESTS

How does a company go about reducing the risk of losing its valuable confidential information and intellectual property? Confidential information must be shared hundreds, even thousands of times each day in the course of doing business. Designing, building, marketing and selling products requires discussing, faxing, e-mailing and otherwise sharing sensitive, proprietary information. Each time confidential information is shared, it is exposed in a way that subjects it to the risk of being lost or compromised.

There is no way to do business and keep confidential information absolutely secure. Rather, information protection is about managing the risk of loss by balancing the company's interest in sharing and protecting information.

FIVE COMPONENT STRATEGY

A comprehensive information protection strategy is based on five key components. Each of these components supports a company's ability to

empower employees and others who work with the company to balance its interests in both sharing and protecting information.

1. Information Inventory

The first component of an information protection strategy requires the identification of the information a company considers confidential. Many companies develop inventories of their valuable information to as a reference for:

- Educating employees;
- Architecting appropriate computer security;
- Determining how to optimize intellectual property value.

2. Policy

Every employee should sign a confidentiality agreement with the company as a condition of employment. While these agreements make clear an employee's obligation to protect the employer's confidential information, the agreement typically does not explain how to fulfill the obligation. An information protection policy should state the employees' responsibilities for fulfilling the obligation to protect the company's information.

3. Communication

Most important to protecting information is communicating to employees, and others who work with the company, so they understand which information is considered confidential and their responsibilities for protecting it. A one-time communication is insufficient. It is far more intuitive to share information than to protect it. Employees who work with confidential information every day get lulled into a sense of familiarity and forget that the information they work with is confidential. Therefore, an effective information protection strategy must include ongoing, attention-grabbing communication to employees and others who work with the company's confidential information.

4. Security Infrastructure

A security infrastructure provides the tools and technical controls to implement information protection. The security infrastructure includes, among other things:

- Firewalls to limit access to computing resources;
- Encryption programs to secure electronic communications;
- Shredders to destroy obsolete confidential documents;
- Nondisclosure agreements for meetings with prospective vendors, consultants and job applicants; and

- Physical security controls, including locks on doors and filing cabinets.

5. Accountability

An information protection strategy will only be effective if individuals with access to a company's confidential information are held accountable for protecting it. To hold individuals accountable, a company must "walk the talk" of the information protection strategy. In many cases, this means changing the corporate culture so that everyone understands that the company takes seriously the expectation that all those with access to confidential information will protect it.

Senior management must lead by example. Employees who violate the policy must be disciplined. Many companies include the responsibilities from the information protection policy in their management objectives and in the performance objectives for all employees.

OTHER COMPANIES' INFORMATION

A comprehensive information protection strategy, consisting of the five components described above, is very effective for managing a company's risk of losing its valuable confidential information. In today's business environment, however, where companies not only share, but often receive confidential information, we must also be concerned with avoiding the unauthorized use of other companies' confidential information.

The Economic Espionage Act of 1996 (EEA) makes it a federal crime to take, download, receive or possess trade secret information obtained without the owner's authorization. Penalties for violation of the law include ten million dollars in fines and fifteen years in prison. It is prudent, therefore, to integrate an EEA compliance program into the information protection strategy. Luckily, an EEA compliance program includes, though it is not limited to, the five components described above.

About the Author

Naomi Fine is an attorney and the President of Pro-Tec Data, a consulting firm dedicated to helping companies identify and protect confidential information. Pro-Tec Data develops and implements information protection programs that incorporate legal, computer security, human resources, and audit protections for information. These programs help companies avoid claims of misappropriation and liability under the Economic Espionage Act. Pro-Tec Data's clients include many of the Fortune 500. Ms. Fine has helped thousands of executives and managers incorporate information protection into their corporate vision and business objectives. She is the author of hundreds of information protection policies, procedures and standards, employee handbooks, training programs and employee communication materials. She has served as both faculty and chairperson for nationwide conferences on information protection and Economic Espionage Act compliance. Ms. Fine is a member of the American Corporate Counsel Association, the American Society for Industrial Security, the Information Systems Security Association, and the Society of Competitive Intelligence Professionals.