

Protect Your Organization's Proprietary Information and Avoid Breaking U.S. Law

Every day companies unwittingly violate U.S. export law. Whether they are transferring technical information to a joint venture partner in a European country or shipping a computer CD to an overseas client, they are potentially putting their own company at risk. The penalties for such errors are daunting, and ignorance of the law is not a defense. For a mere administrative ("civil") infraction, the penalty is up to \$100,000 per occurrence. For intentional misdeeds, which are accorded criminal penalties, well, let's not even go there. Such are the dangers of operating in a global environment.

Few business executives realize that these laws apply to a far wider range of products and technical information than the obvious military armaments. Computer software, including off-the-shelf commercial office programs, is in many cases subject to export controls, as are many other seemingly commercial items having a potential dual use.

The loss of proprietary advantage is an even larger danger. As industrial espionage increases, companies must find new ways to keep their information out of competitor's hands. Interestingly, a recent report out of the U.K. placed France on equal standing with Russia as an intelligence threat, not for military secrets, but rather industrial espionage. Unfortunately, most companies believe these threats only apply to military, space, or ultra-high technology markets. Not so!

Today, businesses in many run-of-the-mill industries are clearly at risk. Worse yet, many still do not realize it, even after they have been stung. Business plans, customer lists, technology, and other strategic assets are often lost or severely compromised without the company knowing it until long afterward, if ever. Have you ever wondered how your foreign competitors suddenly "got so smart" or why they "seem to know every move we make"?

There's no doubt these problems are serious. The question then becomes: Is there a practical answer, short of a paranoia, that inhibits proprietary information loss between customers, competitors, and suppliers alike? Yes! Each company needs certain policies that keep their information from suddenly appearing in the wrong hands. These include:

1. A written policy regarding the exchange of technical data between the organization's U.S. and any offshore company owned or representative offices and personnel.
2. A written policy regarding employees taking technical and business data, both hard copy and electronic, home or downloading it remotely after hours.
3. A written policy regarding what types of technical and business data may be carried on laptop computers and/or downloaded when outside the country.

However, as any executive knows, policies alone are not enough. If the policy is to have any effect, companies must also educate employees and any independent contractors working in the facility not to disseminate any technical and/or commercial information to anyone outside the organization, except on a need-to-know-basis. This includes everyone from the Chairman and CEO to the maintenance staff.

Few companies realize just how much significant information employees reveal at the local watering hole. Merely "hanging out" at the local lunch place or after work gathering spot is an old but tried and true technique that has enabled many competitive intelligence gatherers to learn critical information. It is quite amazing what you can learn from production workers or administrative support staff over a beer or two, especially on a Friday after work. Casual conversation often reveals information such as production problems, order backlogs, customer and supplier names, quality problems, new product developments and strategies, capital expansion plans, hirings, firings, lay-offs, and far more.

In addition, companies must brief management, marketing, technical, and contracts personnel on applicable government technical data export regulations. This mandatory education for all should be standard for new hires, as well as reviewed periodically at company meetings, in newsletters, and through other means. Finally, the executive team should appoint a single Point Of Contact, with an alternate in cases of his or her absence, who must approve the export of any documentation. This includes data released in hard copy, fax, electronically, verbally, and by visit of foreign nationals or during visits to foreign companies or government offices.

Many North American companies underestimate the extent of competitive intelligence gathering that occurs, as well as the detrimental effects it can have on an organization. When companies make a conscious effort to protect their proprietary secrets, they not only reduce their legal liability, but they also assure their company's competitive edge.



John Di Frances is an internationally recognized expert on Strategic Business Issues. His professional career spans thirty years of global corporate, nonprofit, academic and government agency experience in senior executive and industry leadership positions. John advises senior executives globally and is a prominent professional speaker. Since 1983 he has served as the Managing Partner of DI FRANCES & ASSOCIATES, LLC.