

DON'T WAIT UNTIL THE HORSE IS OUT TO CLOSE THE BARN DOOR
a.k.a.
PROTECT YOUR ORGANIZATION'S PROPRIETARY INFORMATION
& AVOID BREAKING U.S. LAW

The other day one of our overseas clients called in a state of near panic, to ask a question. At issue was whether they had unwittingly violated U.S. law by transferring technical information to a joint venture partner in a European country. After hearing a two minute description, I was able to answer a resounding "Yes"! Such are the dangers of operating in a global environment. The worst part is that my client had been lead into their misdeed by following the well intentioned advice of a Fortune 100 U.S. corporation. One that certainly should have known better, but obviously does not. The potential 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.

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 for instance, are in many cases subject to export controls, as are many other seemingly commercial items having a potential dual use.

In addition to the legal dangers, are those surrounding the loss of proprietary advantage through the sharp practice of intelligence gathering by competitors and even industrial espionage. 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 that 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 can be lost or severely compromised without even knowing it until long afterward, if ever. Companies frequently wonder how their foreign competitors suddenly "got so smart" or why they "seem to know every move we make."

Both problems are serious, but is there a practical answer short of a paranoia that inhibits healthy business openness, dialog and partnering with customers, competitors and suppliers alike? Let's look at a simple 5 Point Set of Policies that can effectively protect your organization within just a few weeks and at little or no cost.

1. Education: Every employee of your organization and any independent contractors working in the facility need to be briefed on the requirement 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 can often be parlayed at the local watering hole. Merely "hanging out at the local lunch or after work gathering spot" is an old, but tried and true technique that has enabled many a competitive intelligence gatherer to learn critical information. It is amazing what one can learn from production workers or administrative support staff over a beer or two, especially on a Friday after work. Casual conversation can reveal 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, management, marketing, technical and contracts personnel should all be thoroughly briefed 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 and in newsletters and through other means.

Competitive intelligence gathering and industrial espionage are issues that are seriously underestimated by most companies today, especially in North America.

2. The Leadership should appoint a single Point Of Contact ("POC") with an alternate in cases of their absence, who must approve the export of any documentation. This includes data released in hard copy, fax, electronically, verbally and by visit, either of foreign nationals or during visits to foreign companies or government offices.

3. 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.
4. A written policy regarding employees taking technical and business data, both hard copy and electronic, home or downloading it remotely to work on after hours.
5. A written policy regarding what types of technical and business data may be carried on laptop computers and/or downloaded when outside of the country.

Although not exhaustive, this will form a good basis for beginning a program to guard against export law violations and loss of competition sensitive data.



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.