Reprinted with permission from Security Technology & Design, January/February 1997

Economic Espionage, Proprietary Information Protection: The Government is Here to Help You - Seriously

In the 1970's and 1980's, we had a difficult time getting law enforcement cooperation and prosecutorial interest in what were - at that time - termed "crimes involving computers."

Law enforcement tended to view such "crimes" as a gaggle of geeks sitting around and doing terrible things to small furry bits and bytes. They were not considered real crimes, since there was rarely anybody to arrest with the goods. Smoking guns were rare. No real lawman would bother investigating something like this. And, it was altogether far too complex to understand, let alone waste time bother investigating. With outrageous caseloads, who had the time?

Prosecutors were even more difficult to bring into the loop. They not only had essentially the same "anti-geek" biases, they had a somewhat more difficult problem in concept. What laws were actually broken and how? The best we could do after lots of handwringing and headbanging might be a prosecution under wire fraud statutes. Again, what prosecutor had the time to get smart enough to be able to convince a jury box full of non-rocket scientists that a dirty deed had been done? Most often, the answer was an appeal to the legislative branch: "If you folks think this is such a big deal, why don't you get the city council, the state legislature, the US House and Senate, or Mothers Against Cracked Eggs to enact some legislation?"

Indeed, since money is what really makes the legislative wheel turn every once in a while, it was the large dollars that victims were beginning to lose that changed the law enforcement, prosecutorial and lawmakers attitude. Victims such as large banks, investment houses and many other organizations where electronic transfers were becoming the favorite target of computer literate criminals. Their response was in the form of influencing their legislators to provide what they needed in the way of legal recourse. In the past two decades, there has been a steady rise in the number of legislative fixes to help companies and government entities protect their information. It has also spawned a whole new career field for cyber-cops and D.A.'s who are no longer electronically challenged.

On October 11th, 1996, the Economic Espionage and Protection of Proprietary Economic Information Act of 1996 was signed into law, with considerable bi-partisan support. This new legislation represents an attempt by the Federal government to apply some of its strength against problems that are costing American business billions (that's with a B) of dollars each year. As had been the case with the computer crimes of a few years ago, this is legislation which represents a good start - but not an end point - since the changes in the world rarely wait for the Congress to anticipate them. And, as in the case of the computer crimes legislation being prodded by bucks, a fair amount of lobbying money was directed towards this effort. As just one example, IBM included in its reports to the Clerk of the House Representatives that it had spent $2,680,000 in the first six months of 1996 on

its lobbying efforts on various issues, specifying the Economic Espionage Act among them.

Focus of the Act

This new law has two primary elements, neither of which have ever been previously, specifically covered by US law.

First, it allows the national counterintelligence apparatus - mostly the Federal Bureau of Investigation - to be brought to bear on the activities of foreign intelligence services. They've always had a responsibility to confront and neutralize the collection efforts of hostile intelligence services, but only against classified government information and programs. This law allows them to investigate cases where a foreign intelligence service - using tried and true intelligence principles that have worked in international affairs for years, decades, and even centuries - attacks American firms in order to gather information of a proprietary nature. Information that they gather in order to further the commercial interests of the firms in their countries.

During the Congressional hearings, and in testimony ever since Senator Cohen (R-Maine) introduced it in January of this year, various officials have painted a picture of the size and nature of the problem. From FBI Director Louis Freeh's perspective, no less that 23 foreign countries - ranging across the globe from the French to the Japanese and Russians - are actively engaged in economic espionage operations against American firms. His perspective is based on the doubling of the FBI's caseload for this kind of investigation, from 400 to almost 800, in just the past year alone.

And, what is it that they're after? They're after technologies that are being developed in the United States, where the government spends almost $250 billion and private industry spends another $300 billion. It doesn't take the President of the World Bank to figure out that if you spend $500,000 bribing a research scientist in the United States to get the trade secret or proprietary information that an American company has spent $750,000,000 developing, the intelligence operation has just netted $700 million. Even in government terms, $700 million is a noticeable amount.

Dan Swartwood, Competitive Information Security Manager at Compaq in Houston, attempted quantify what actual losses American businesses suffered. Swartwood, under the auspices of the American Society for Industrial Security, conducted two surveys - one in 1992 and one in 1995. Swartwood's data revealed that "potential losses for all American industry could amount to $63 billion for the reporting period (1993-1995) or about $2 billion a month." Swartwood's study, in which he was assisted by ASIS' Dick Heffernan, also showed that the average loss for the 700 incidents reported by 113 respondent companies was $19 million, $29 million and $36 million in high technology, services and manufacturing sectors respectively.

Second, the Act also redefines the phrase "goods, wares or merchandise" to include the term "proprietary economic information" of a company in Federal laws relating to stolen property. Thus, it extends the definition to allow Federal investigation and prosecution in the event that the misappropriated information is used in interstate commerce.

Overall, the Act - for the first time - truly links economic well-being of the Nation to national security interests. This Act validates, finally, an argument that many have been making for years: theft and misappropriation of company proprietary information ultimately "directly and substantially threatens the health and competitiveness of the US economy and, consequently, the Nation's security." Additionally, it also provides for Federal relief for those firms who have been victimized by having their information stolen and then transferred out of the jurisdiction of existing State laws in

much the same way that the Federal computer crime statutes have been built over time.

Is This A Panacea for All The Problems?.

Hardly. Indeed, this legislation is best viewed as a good start in efforts to deal with an ever-increasingly complex set of problems for corporate leaders, and especially for the security management team responsible for protecting and covering their assets. Indeed, it would be an unwise security manager - or company leader - who thinks that his problems have all been solved by the intervention of the Federals. Some examples of possible problems.

Section 576 of the Act relates to confidentiality. The intent of this section is - apparently - to make offended companies more warm and fuzzy about prosecuting cases through the Federal system. It provides for a court to "preserve the confidentiality of alleged proprietary economic information by any reasonable and lawful means." Anyone who has been to a county fair and a goat roping knows that what a judge - on any given day - decides is "reasonable and lawful means" is not something you want to bet the ranch on. This is especially true when lawyers involved in multimillion dollar lawsuits are equipped with $500 an hour silver tongues.

This section of the law becomes even slightly more problematic when we pay some attention to the last sentence: "Any owner of the proprietary economic information which is the subject of the offense may request the prosecution to seek such protective action." (Italics added) And, if the prosecution simply declines to respond to the offended company's request? What protection is there then?

Please bear in mind that you are not reading an article written by a lawyer. But, on the other hand, remember that you are reading an article written by someone who spends every working day involved in the collection and analysis (or the prevention of collection by others) of competitively valuable information. One of our favorite places to look for information is in court records, because discovery proceedings often yield more about a particular firm's business secrets than were alleged to have been misappropriated in the first place.

We Feel Your Pain

There are two ways to view pain in this situation.

The first is the amount of suffering that a person or corporation is exposed to as a result of being found guilty of violating this Act. For an individual at the worker-bee level, the fines max out at $1,000,000 and jail time at 25 years, or both; for officers of corporations, they can receive fines up to $5,000,000 and jail up to 25 years, or both; and, for corporations, fines can reach up to $50,000,000. Regular readers of this series of articles on Countermeasures to Competitive Intelligence, Industrial Espionage, and international commercial espionage, will see that this Act has considerably greater potential deterrent impact than described in "You Don't Have to Be General Motors To Be A Target." Those readers will recall the instance of the young French software engineer cum espionage asset who got to perform 1,000 hours of community service in his homeland instead of jail time in California where he had done the evil deeds.

The other way to view pain in this situation is to look at how the victim's pain is alleviated. Fines, forfeitures and jail time for the miscreants are all well and good, but if you think that's going to help ease your pain, you haven't dusted for the trial lawyers' fingerprints yet. They're there. This Act doesn't necessarily mean immediate relief for your firm. Indeed, Section 573, the Act calls for all

amounts from the forfeiture of property by a violator to be deposited in the Crime Victims Fund of the Victims of Crime Act of 1984. (Italics added) That means it goes into a pot - one in which you may or may not share. After administrative costs, naturally.

So, in order to get any of your money back, the civil courts have to provide for your relief. Clearly the task will be made much easier by a conviction in the criminal proceedings. But, how much is your civil case compromised if the offending company is found not guilty in the criminal trial. Perhaps the outcome of O.J.'s civil trial will give an insight.

Who's Minding the Store?

You are. Of course, that's nothing new. The security management team is always responsible for employing countermeasures consistent with the level and type of threat against the firm and its property, whether intellectual or not. This legislation does nothing to change that. Just because there appears to be some significant Federal involvement in this, that doesn't mean it extends out to actual protection.

It's not up to the FBI, the DEA, the Commerce Department or even the Fish and Wildlife Commission to protect your proprietary information. As the Act specifically states, protection is only extended to proprietary economic information when the "owner thereof has taken reasonable measures to keep such information confidential." Further, this Act seems to suggest that you must first convince the enforcement agency that you've done what you needed to do, consistent with the present threat environment, to protect your information.

Requiring that a company have "taken such reasonable measures" to protect its information seems far less complicated than brain surgery. After all, doesn't everybody understand that? Doesn't everybody do it? Sadly, the answer in four out of five cases where we are asked to assist in a trade secret misappropriation case, intellectual property theft or questionable Competitive Intelligence case, the answer is "No." And not only, "No", but often "Heck, No."

Space doesn't permit the listing - let alone the explanations - we have heard over the years. But, suffice it to say that a company that is looking to recover lost revenues through the courts - and hasn't ever done anything to really protect themselves from the changing dynamics of the marketplace - has a better chance at the lottery.

Sadly, the most that some companies can do once the secret is out of the R&D lab is to design ways to deal with those threats in the future. Often, by the time a company knows that this has to be the way to conduct its business operations in the future, myriad complicating factors have entered the equation. A corporate culture of complete openness and trust for all living creatures is often just one of the many.

A final point of concern from a cognizant security manager's perspective relates to stockholder equities. Since this legislation appears to mandate - for the first time - that companies actually take the active measures necessary to protect themselves from such losses, it opens a whole new set of potential liability issues from a due diligence perspective.

Related Article: Economic Espionage Act Update

Back to Library

About the author: John A. Nolan, III CPP, OCP is Chairman and Managing Director of Phoenix Consulting Group, which provides competitive intelligence, counterintelligence and professional development/training programs across a variety of industries. He is also a co-founder of The Centre for Operational Business Intelligence in Sarasota, FL where corporate intelligence practitioners from around the country and the world learn the tools and techniques necessary to prevail in the marketplace. His newest book, CONFIDENTIAL: *Uncover Your Competitor's Top Secrets Legally and Quickly - And Protect Your Own* was released by HarperCollins Business Books in June 1999. He is frequently featured in national and international media such as Forbes, George, Times of London and CNN, to name just a few. He can be reached at mailto:jnolan@intellpros.com, or at 1.800.440.1724