Reprinted from Security Technology & Design, August 1997

Economic Espionage Act Update: Good Guys 1, Bad Guys 0

The author answers the many questions from readers curious about the Act's impact on their businesses

Without question, my January 1997 article on the Economic Espionage Act of 1996 has elicited more questions than any other article in this series. Questions came from both security managers who wanted to know specifically how it related to them and their companies as well as General Counsels who wanted to know just about everything - without admitting that they didn't know it all already.

Perhaps the most persistent questions related to who was being charged under the statute and what the outcomes had been; less often, but still prevalent were those who wanted to know what they needed get started on a case. Now that the jury is back with the verdict on the first case brought under the Act, a review of that case maybe helpful for today's security manager.

In November 1996, within a month of the passage of the EEA, Glenn H. Hiner received an interesting fax. That's not unusual, since as the Chairman and Chief Executive Officer of Owens Corning in Toledo, he gets lots of interesting and important faxes. This one stood out. The fax - poor spelling notwithstanding - offered to sell many specific kinds of information relating to the operations of PPG's Research and Development Center. Information which the fax claimed would be worth millions of dollars to PPG. Information that included CAD/CAM drawings, blueprints and a whole laundry lists of other items of importance. Information which certainly appeared to be credible and important. Information that was clearly illegal to transmit from an employee of one company to the CEO of another.

It wasn't long before Owens Corning's General Counsel was calling his counterpart at PPG in Pittsburgh to tell him the good news. PPG's General Counsel knew exactly who to turn to next: Regis W. Becker, the Director of Corporate Security.

Becker, an ex-FBI agent who had just completed a year of service as President of the American Society for Industrial Security, Becker was in an ideal position to know the lay of the land - including the recent passage of the EEA. The case that seemed to be the kind of classical industrial espionage that the Act was intended to prosecute. Indeed, it turned out to be the first one, even though the FBI Director Louis Freeh had testified during the hearings prior to the passage of the Act that the Bureau had 600-800 open industrial and economic espionage cases.

Becker's first call was to the local FBI office in Pittsburgh, specifically to the Foreign Counterintelligence (FCI) squad. It seemed natural to assume that since the FBI's ANSIR program (then recently renamed from the previous DECA program) was the province of the FCI squad, investigations under the EEA would be their job. Unfortunately, the Act was so new that even many of the people in the Bureau hadn't sorted it out yet. It took a week or so to learn that it was, in reality, the job of the White Collar Crime investigators as opposed to the FCI squad. Things happened

rapidly after that though.

Within days the Pittsburgh and Toledo offices had collaborated in setting up the FBI's response, which began with a call from the Toledo office to the response number on the fax. Days went by without any calls from the seller of the secrets - until the Law of Friday Afternoon was applied. That's when the call came in, naturally. A meeting was set up for the following morning outside Pittsburgh.

Saturday's meeting had not only its two principals, but also its support cast. The FBI surveillance team was in place; so was the secret seller's brother who was there for exactly the same purpose, but without a badge.

Within minutes it was clear that Patrick Worthing, a 27 year old temporary contract worker at PPG's Research and Design Center had good samples of the items he had for sale. When the money and secrets traded hands, it was time for Worthing, and his 30 year old brother Daniel, the surveillant, to put on their new bracelets. And brother Daniel wasn't the only family member who got involved: the fax station identifier was tacked back to the company where his wife worked, although it was later fairly clear that she was not involved in the attempt.

Beyond getting involved in this criminal activity, Worthing was a bright enough fellow, and a good worker to boot. Brought into PPG originally as a temporary line worker, he was soon promoted to supervising a number of other temporary contract workers at PPG's pilot production facility at its Research and Development Center. In that capacity, he had access to a wide range of proprietary information: fax transmissions, drawing and prints, and even diskettes containing electronic versions of the data. And, he'd been systematically collecting the information for the ultimate purpose of selling it to someone for quite a while before he sent his fax to Owens-Corning.

After his arrest, he gave two possible explanations for his actions: one, he wanted to compile information that he could use as an insurance policy against the day that - as a temporary worker - he would inevitably leave PPG; or two, that he wanted to get back at PPG for his treatment as a second class citizen - a common complaint among temporary workers - in comparison with other, permanent PPG employees.

Neither issue, however, had much to do whether or not he was guilty. Both he and his brother were found guilty. They'll both soon be coming to a Federal institution near you for an eighteen month engagement; and their fines were $1500 apiece. Although the sentences and fines were nowhere near what they could have been, they nonetheless sent a clear signal that breaking the new Federal statute would be dealt with much more severely than breaking state trade secrets laws had been in the past.

This is not to say that the sentences were yet fully commensurate with the potential damage the pair might have caused. Indeed, the statute requires an assessment of the actual or potential loss: in this case, the potential loss was calculated by PPG to be in the range of $20-30 million had it been actually transmitted to and used by a business rival. Obviously, the sentences would have been closer to the maximum penalties for violation of the Act (up to $500,000 and/or 15 years for individuals, and $10,000,000 for organizations) had there actually been a transfer of the information to someone who could've used it for competitive advantage.

There's Nothing Really New Under the Espionage Sun

There are lessons to be drawn from the parallels in this case with many other espionage cases;

lessons that the counterintelligence community has talked about in government security training programs for years:

1. Spies, and even industrial spies, are rarely seen wearing cloaks or slouch hats: they look like any average person.
2. Spies rarely advertise that they are disgruntled or displeased with their role in an organization they are betraying; they usually look like successful and dedicated employees.
3. Spies typically underestimate the effectiveness of security or counterintelligence personnel to neutralize their efforts; they tend to think of themselves as superior to the forces or truth, justice and the American way.
4. Spies underestimate the honesty and integrity of others; they think that those to whom they want to communicate the information are as venal as they are.

And, since many are quite familiar with the case of John Anthony Walker and his decades long espionage activities on behalf of the Union of Fewer and Fewer Republics, we can see some of the other characteristics of those who would commit espionage:

1. A willingness to involve others in their treachery - both wittingly as in the case of the brother as well as unwittingly as in the case of his wife.
2. Amateurs will always do amateurish things and they'll get caught at it.
3. That had the espionage actor followed traditional intelligence tradescraft, to include personal and operational security, the outcome might have been considerably different.

For those who read about this and have an idea that PPG still remains a potential target for industrial espionage, if done "correctly", there has been a considerable change in the landscape at that company. Just as one of the better definitions of a conservative is that he or she is a liberal who got mugged last night, corporate leadership's responses to the potential at PPG was swift and unequivocal.

Within days of the alert from Owens-Corning, a corporate wide, security and counterintelligence audit was underway with heavy emphasis from mahogany row. But then again, almost every security manager with more than an hour of experience knows that it sometimes takes pain to get leadership to respond to what they've been warned about in the past. In the past, at PPG, there had been good support all along. So, if there's a lesson to be learned here it sounds like a Robert Shuler title for our business: "Sometimes bad things happen even in good security programs." Is it time for that top to bottom review you've been thinking about doing. Is now the time to get that leadership support for making the security program more aggressive?

So far in this series we've spoken about competitive intelligence (as practiced mostly by fairly ethical people using legal yet highly effective means), industrial espionage (as practiced on behalf of one country against a small California firm), industrial espionage (as practiced by a walk- in type employee in the PPG case) and about countermeasures to deal with these variants on a basic theme. A basic theme that is more and more current with each passing day as business gets more and more competitive and as companies and countries do more to gain an edge than they've been willing to do in the past.

And, just to peak your curiosity a bit more, there's an interesting little case taking shape under the Economic Espionage Act in Pennsylvania. It came to light as this article was being completed.

It seems that a Taiwanese (remember boys and girls they're the ones who are our friends off-shore)

national by the name of Kai-Lo Hsu Hsu was arrested on June 16, 1997 for attempting to steal pharmaceutical related trade secrets. Mr. Hsu is employed as the technical director at Yuen Foong Paper Company Ltd, in Taipei.

Now, on its face, the first question that inquiring minds want to know is "Why in the dickens does a paper company want pharmaceutical trade secrets." Maybe the simultaneous arrest of one of his countrymen in the same case will help pull this together a little. The second person arrested was Professor Charles Ho, from National Chiao Tung University in Taiwan: he is also a co-owner of Asiapharm, a biotechnology firm located in Delaware. It seems that Bristol- Myers Squib was really unwilling to share the plant cell culture technology that is used to manufacture the ovarian cancer fighter, Taxol. Imagine.

In any event, odds are that the penalties may be a little stiffer in the Bristol-Myers Squibb case than in the PPG case. The actual charges against Hsu are attempted theft of trade secrets, conspiracy to steal trade secrets, and other violations; Professor Ho can add charges of aiding and abetting interstate and foreign travel to commit bribery, along with conspiracy, to his curriculum vitae. Bear in mind that the new law allows for many years in a Federal Guest Quarters, and the potential for millions of dollars in fines when companies are actually involved. Since this will be the first foreign linked case prosecuted under the Act, it will set the stage for those that follow. Things may get interesting.

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
