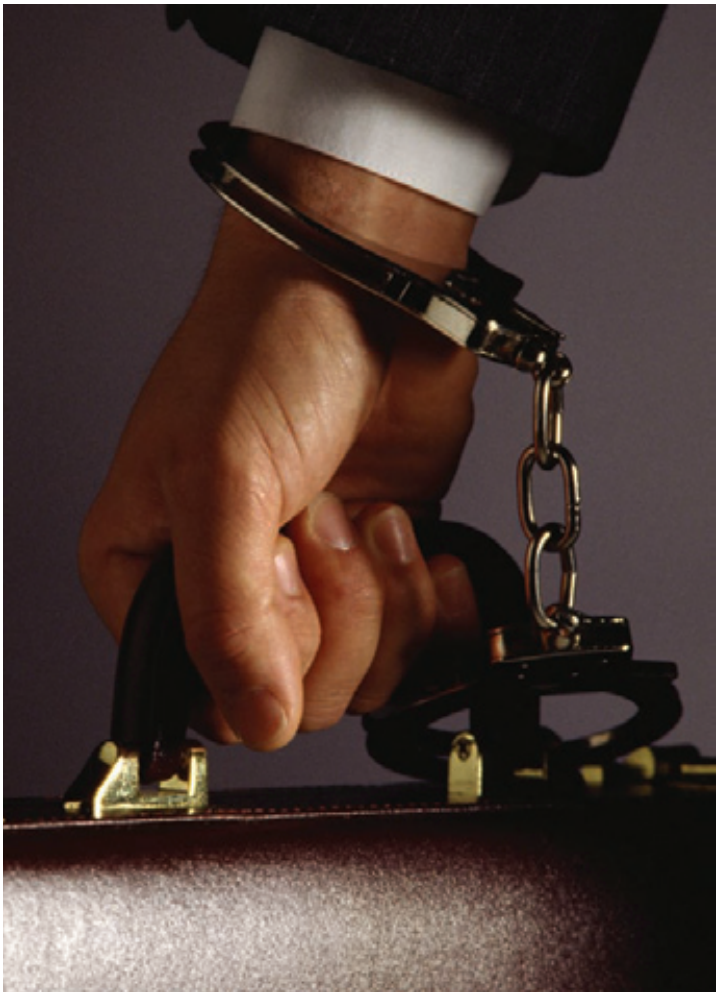
ESPIONAGE: Real Warfare on American Business

By Michael Kennedy, CPP

Warfare—that's business these days. What a great metaphor for the strategic thinking and bold actions of business today. This legal and healthy competition benefits us all.

Did you know that today there is another kind of warfare on American business that is not metaphorical? It's all too real, and it's a dirty business. This warfare is destroying the wealth of individuals, the jobs of all too many, and it is compromising our national security. In this war the battles are often unseen, until it is too late. Many victims never even knew they were in a war – that is, until they find themselves numbered among the defeated.

These are the realities of economic and industrial espionage, an illegal activity that costs American business billions annually. WARNING: This article is not about defense or national-security-related industries.



It is about stealing the formula for a new self-adhesive, pharmaceutical or razor blade design. It's about YOUR business, not someone else's.

Ask Avery Dennison or Ellery Systems about their experience with economic and industrial espionage. Actually, you can't ask Ellery Systems. They went from cutting-edge brilliance to non-existence because of an economic espionage attack. As one writer put it, "Man-centuries of incredibly complex and hard work and millions of dollars of investment were lost to a foreign country." Ellery lost proprietary information worth tens of billions of dollars in the marketplace. It is a classic case, and tragic one. We should all read the classics from time to time.

You cannot ask Ellery Systems, but you could ask Eastman Kodak, Gillette, or Bristol-Myers Squibb. These businesses were all victims of economic and industrial espionage.

If you know this threat to your business, and you are taking real countermeasures to protect the intellectual capital that comprises as much as 75 percent of your company's value, your source of wealth creation and revenue, and those countermeasures are proportionate to the value of the asset, then good for you.

If not, or if this is news to you, or you thought information security was only IT stuff, then brace yourself.

No Kidding

Someone is saying right now – "You're kidding! Espionage is for movies and paperback novels." My friend, that is simply not true today. Without sounding like an alarmist, I hope to share enough about this issue for you to pursue the matter in your own research. Do that and you will find out more than you ever wanted to know. Then you can be the alarmist where it counts.

Incidentally, I'll address only the foreign collection of American business intellectual property. Domestic economic and industrial espionage is a significant issue too but that's for another day. The looting of intellectual capital by foreign entities, whether they are backed by a foreign government or not, is plenty for today.

The Situation

Richard Hefferman, in testimony before the US House of Representatives on May 9, 1996, cogently

described the situation facing American business:

> *Mr. Chairman, I want to thank you for inviting me here today to testify with regard to the extent and severity of economic espionage affecting our nation's interests. More than that, I want to thank you and the members of your Subcommittee for helping to open a public dialogue on this issue. For the greatest danger to our nation today is not, in my opinion, on the military battlefield, but in the complex and shadowy world of economic and industrial espionage.*
>
> *Who is at risk? If you have a competitive advantage over others in the products or services that you develop, manufacture or supply, your business and technical information is at risk from those adversaries who are seeking unearned competitive advantage by the fastest means – theft of your intellectual property. We are in an era where the national interests of global competitors are increasingly focused on achieving an unearned advantage over their competitors at almost any cost.*

That testimony was a decade ago. Shortly afterward, Congress passed the Economic Espionage Act of 1996.

Of course, that was before 9/11/2001. Terrorism, espionage designed to steal defense technology, and the proliferation of WMD's now rightly top the FBI's Counterintelligence National Security Threat List of eight issues. Guess what's #4? That's right: Economic Espionage. It is second only to the threats that would literally kill us.

Read Dick Heffernan's statement carefully, take it for face value, and you will know what you need to know.

The Big Change

Hefferman said, "We are in an era…" as if there was something different about this era when compared to a previous one. Actually, something changed when the Soviet Union collapsed and the US became the lone military superpower. As early as 1992, Robert Gates, former head of the CIA, describes the change in testimony before the US Congress:

Suggested Resources

Links:

The Office of the National Counterintelligence Executive
www.ncix.gov/about/index.html

American Society of Industrial Security IAP Council (toolkit)
www.asisonline.org/councils/SPI.xml

Texas A&M University Research Foundation Employee Guide to Security Responsibilities
rf-web.tamu.edu/security/secguide/Home.htm

Chief Security Officer Magazine Online (Secrets Stolen Fortunes Lost)
www.csoonline.com/read/exclusives/secrets fortunes.html?source=darwinobserver

Federation of American Scientists
www.fas.org/main/home.jsp

Print:

The Quiet Threat by Ronald L. Mendell

Confidential by John Nolan

War By Other Means by John J. Fialka

Enemies by Bill Gertz

Sticky Fingers by Steven Fink

Our fundamental assessment is that, while the end of the Cold War did not bring an end to the foreign intelligence threat, it did change the nature of that threat. The threat has become more diversified and more complex. In a world that increasingly measures national power and national security in economic terms as well as military terms, many foreign intelligence services around the world are shifting the emphasis in targeting. Foreign targeting of American technology continues; technology is important for economic as well as military reasons. Since the U.S. continues to be on the cutting edge of technological innovation, technology theft will remain a major concern for us.

After the Cold War, many foreign national intelligence services, who previously were focused on military and national security issues, began to emphasize economic and industrial espionage to support their nation's economic competitive position.

In 1994 The National Economic Council reported, "Economic espionage is becoming increasingly central to the operations of many of the world's intelligence services and is absorbing larger portions of their staffing and budget." Same spy techniques and spies, with different targets – American business.

Former Director of the FBI Louis Freeh, on February 10, 1999 (USA Today: FBI: Spies Cost U.S. Firms $2B per Year), said:

U.S. companies are under economic attack from 23 countries trying to steal trade secrets and other intellectual property in the most severe threat to national security since the Cold War.

Director Freeh also said before Congress that "foreign governments ... actively target U.S. persons, firms, industries and the U.S. Government itself to steal or wrongfully obtain critical technologies, data and information in order to provide their own industrial sectors with a competitive advantage."

Kind of grabs your attention doesn't it – considering the source.

This very day, the Texas A&M's Research Foundation Security Office Guidebook states, "Foreign intelligence services and corporations are increasingly using classical espionage techniques to steal U.S. corporate marketing information, technological advances and proprietary data in support of their national economic goals."

It's Not Getting Better

Imagine – 23 nations targeting U.S. Business.

How about this one? A mere five years later, in its 2004 annual report to Congress regarding foreign collection of U.S. economic and industrial proprietary information and trade secrets, the National Counterintelligence Executive (ONCIX) reported that over 100 foreign countries were identified as involved in such attempts that year! In a 2005 speech, the same NCIX indicated that some "140 nations and some 35 known and suspected terrorist organizations currently target the United States for intelligence collection." Is it just me or is the number increasing dramatically?

The Way to Beat America

John J. Fialka calls economic and industrial espionage the "War by Other Means." Espionage was long seen

George Washington, the Father of Our Country, left us with this admonition that we would do well to heed:

"There is one evil I dread, and that is their spies. I could wish, therefore, that the most attentive watch be kept..."

as the most cost effective way to overcome America's military superiority – now it's the method of choice to overcome our economic superiority. Many countries see American business as the world's smorgasbord for the innovation in goods, services, research and techniques that they need to compete with us in the global marketplace, and they will do things you would never do to get them.

It is no longer simply the U.S. against another country – i.e. Spy vs. Spy. Now it may well be an individual American business against another country – a sovereign government, including its professional intelligence apparatus – Junior Research Assistant, File Clerk, Machinist or your suppliers vs. Professional Spy.

When they succeed, America's businesses literally compete against themselves and fund the entire project.

Implications and Action

Consider the implications of what you have read. John Conway said, "The two most common reasons for losing are not knowing you are competing in the first place, and not knowing with whom you are competing." Before you read this ,if you did not know you were competing, you know now.

Do you fit Hefferman's "Risk Factors?" Do you "have a competitive advantage over others in the products or services that you develop, manufacture, or supply?" Are you working on it? If so, then YOUR business is a potential target of economic and industrial espionage. It's no more difficult than that.

The good news is that much can be done to protect our intellectual property from espionage. We will only succeed if we, individually, take the threat seriously and are willing to take appropriate countermeasures to protect what is rightfully ours. We are not helpless at all, if we choose to deal with it.

Forewarned is forearmed. When you have too many fires, you may have an arsonist.

Our adversary is more than willing to break in and steal all that you and I are working for just to gain an unearned competitive advantage against us. When it's gone …well, you know the rest.

Such is the truth of our era of business warfare. **N**

Michael Kennedy, CPP. Michael is the quality and safety manager for SETEC Protection Service in Houston,Texas and a member of the Information Assets Protection Council of the American Society of Industrial Security International. Michael can be reached via email at mkennedy@setecprotection.com.