How to Respond to the Threat of Corporate Espionage

Presented by Audra A. Dial & Clay C. Wheeler

September 26, 2013
Corporate Espionage in the News
75% of trade secret theft is the result of an insider attack.

Estimates range from $200-$500 billion lost to U.S. companies each year from corporate espionage.

There is a noteworthy increase in the number of state-sponsored threats.

The methods of accessing targets are widening beyond companies’ own systems to include their trusted advisors (including law firms, consulting firms, etc.).
To qualify as a trade secret, an asset must derive economic value from not being generally known and be subject to reasonable degrees of protection.

Securing confidential information is equally important. IP assets that do not rise to the level of trade secrets can still be protected as confidential information through NDAs and possibly through statutory protections.
General Strategies to Protect Information

- Employment agreements.
  - Ensure employees understand their obligations clearly.
  - Expressly authorize use of electronic information as narrowly as possible.
  - Confidentiality restrictions.
  - Narrowly tailored covenants.

- Computer log-ins and passwords.
  - Restrict levels of access on need-to-know basis.

- Confidential designations, legends, and markings on all confidential information.

- Security cameras, badges, restrictions on access.

- Keep secret information under “lock and key.”
The Federal Crime of Corporate Espionage

• 18 U.S.C. §§ 1831 and 1832 prohibit theft of trade secrets by persons or business entities with:

  Knowledge or intent that the theft will benefit any foreign government, foreign instrumentality, or foreign agent, or

  Knowledge or intent that the theft will benefit anyone other than the owner of the trade secret, and knowing the offense will injure that owner.

• Benefit requirement for trade secret theft is limited to “economic” benefit.

• Statutes reach overseas conduct.

• Federal jurisdiction for trade secret theft depends on trade secret “related to a product or service used or intended for use in interstate or foreign commerce.”
Criminal Prosecution Case Study: 
*U.S. v. Sinovel Wind Group Co. et al.*

- Victim AMSC’s software regulates flow of electricity from wind turbines.
- Sinovel key customer.
- Recruitment of AMSC employee.
- AMSC discovers modified code in China.
- Sinovel exported turbines to U.S. containing software.
Criminal Prosecution Case Study:  
*U.S. v. Sinovel Wind Group Co. et al.*

- Alleged loss in excess of $800 million.
- Called “attempted corporate homicide” by the U.S. Attorney.
- One defendant headed engineering department in Austria, other two individuals in China.
Increased Criminal Penalties

- Foreign and Economic Espionage Penalty Enhancement Act of 2012—maximum fine for an individual is $5 million and for an organization is greater of $10 million or 3 times the value of the secrets.
- Trade Secret Clarification Act of 2012—expanded protection of trade secrets to include secrets that “relate to a product or service used or intended for use in interstate or foreign commerce . . .”
Techniques of Corporate Espionage

- Theft by an insider (esp. current or former employee).
- Exploiting lax password management.
- Email spam.
- Manipulation of supplier/customer relationship.
- Aggressive collection of public information.
Prevention of Corporate Espionage

• Remind employees of confidentiality obligations and what information is confidential.
• Audits of compliance with corporate policies.
• Central monitoring of electronic access to information.
• Monitor Internet postings and blogs.
• Password security.
• Global employee “tip line.”
• Anti-eavesdropping techniques.
Holistic Approach to Preventing Attack

- Conduct risk audit to determine most valuable assets and those most vulnerable to attack.
- Educate cross-functional teams to understand warning signs and remain vigilant.
- Remind employees about protection measures and ways to prevent misuse.
- Take swift action when vulnerabilities/threats are identified.
Internal Investigations

• Why conduct an internal investigation?
  – Identify problems with internal controls.
  – Identify and discipline bad employees.
  – Satisfy disclosure obligations to shareholders, governments or others.
  – Prepare for disclosure to law enforcement.
To Report or Not to Report?

• The determination of whether to involve the criminal authorities can be complicated:
  – Loss of control of the matter.
  – Subjecting company to government subpoenas and interviews.
  – Risk of disclosure of the trade secret.
  – Increased resources of federal law enforcement.

• The first consideration is how to protect the client from any potential criminal exposure.
Civil Prosecution Options

- State Trade Secret Statutes
- State Business Practices Acts
- Conversion
- Unfair Competition
- Breach of Employment/Confidentiality Agreements
- Tortious Interference
- Civil RICO or CFAA Claims

- “Pattern of Racketeering” requires two or more predicate acts such as mail/wire fraud, false statements, interstate transport of stolen goods, criminal copyright infringement.
- “Enterprise” includes any individual, partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact although not a legal entity.
- “Injured in his business or property” requires actual, quantifiable injury to business or property.
Computer Fraud and Abuse Act ("CFAA")

• Provides for civil and criminal remedies against any person who “knowingly and with intent to defraud, accesses a computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value.”
How Broad Is the CFAA?

- **Agency/Broad**: Did the employee use the computer for a disloyal or wrongful purpose or go beyond his employer’s access restrictions, even if he was authorized to use the computer for certain purposes? (1st, 5th, 7th and 11th Circuits)

- **Plain Language/Narrow**: Did the employer authorize the employee to use the computer? (2nd, 3rd, 4th, 9th Circuits) This interpretation is gaining ground.
“Exceeds Authorized Access” – Narrow View

United States v. Nosal
676 F.3d 854 (9th Cir. 2012)

- Employee left Korn Ferry to start his own competing company and had entire client contact database downloaded for use in his new company.
- *En banc* decision finding no CFAA violation because the statute was intended to prevent “hacking” and the violation of an internal computer use policy was too broad to criminalize. The CFAA was not meant to criminalize an employee’s “g-chatting with friends, playing games, shopping or watching sports highlights” in violation of computer use policies.
“Exceeds Authorized Access” – Narrow View

WEC Carolina Energy Solutions LLC v. Miller
687 F.3d 199 (4th Cir. 2012)

• Facts similar to Nosal (employee downloaded confidential information/trade secrets days before leaving to join a competitor).

• CFAA intended to target hackers, not disloyal employees.

• CFAA only applies “when an individual accesses a computer without permission or obtains or alters information beyond that which he is authorized to access.”
United States v. Rodriguez
628 F.3d 1258 (11th Cir. 2010)

- Employee of the Social Security Administration with access to sensitive personal information, such as social security numbers, was charged with violations of the CFAA for accessing the SSA database for personal reasons.

- The court held that the employee was “not authorized to obtain personal business information for non-business reasons” and thus “exceeded his authorized access and violated the [CFAA].”
Civil Prosecution Case Study: Phonedog

• Trade secret misappropriation claim against former employee who converted @PhoneDog followers to @Noahkravitz followers upon departure from Phone Dog; trade secrets are Twitter followers.
• Motion to dismiss denied.
• Case settled; Kravitz maintains custody of the Twitter account.
Civil Prosecution Case Study: Alpha Tire Systems

- Former marketing manager of Alpha Tire Systems conspired with competitor to steal blueprint for unique mining tire.
- Alleged copyright infringement, trademark infringement, unfair competition, conversion, conspiracy, etc.
• Starwood alleged that Hilton induced Starwood employees to serve as corporate spies to provide Hilton with Starwood’s confidential development plans and business opportunities for its luxury brands.

• Alleged theft of 100,000+ electronic files.

• Preliminary & permanent injunction; court monitors appointed until 2013; ongoing criminal investigation.

§ 1337 of Tariff Act authorizes the ITC to halt importation of goods if their production is the result of unfair trade practices.

Companies typically bring cases to the ITC under § 1337 to challenge importation of goods that infringe a patent.

*TianRui* held that these remedies also extend to trade secret misappropriation.
Amsted Industries manufactures cast steel railway wheels.

Amsted alleged that TianRui, a Chinese company, had misappropriated Amsted’s trade secrets to manufacture cast steel railway wheels for importation into the U.S.

The alleged misappropriation and use of Amsted’s trade secrets occurred exclusively in China.

The court held that the ITC may “apply domestic trade secret law to conduct that occurs . . . in a foreign country.”
Criminal Prosecution Options

- Economic Espionage Act of 1996
- National Stolen Property Act
- Wire Fraud
National Stolen Property Act

- **Violation requires:**
  1) Transportation in interstate or foreign commerce of
  2) Goods, wares, or merchandise
  3) That the Defendant knew were stolen, converted or taken by fraud.

- **18 U.S.C. § 2314**
Criminal Prosecution Case Study: Victim Dow Chemical

- Former Dow Chemical Co. scientist stole trade secrets and confidential and proprietary information pertaining to Dow’s CPE process and product technology and conspired to sell the technology to various Chinese companies.
- Convicted by a jury and sentenced to five years for selling the rubber-making secrets obtained from Dow and lying under oath.
- Affirmed on appeal, despite error concerning defendant’s expert (U.S. v. Liu (5th Cir. 2013)).
Two Wyko engineers secretly photographed equipment in Goodyear’s Kansas factory to use in creating a similar device for Chinese customer.

Convicted by jury of, *inter alia*, trade secret theft, conspiracy, and wire fraud.

Wyko employee tipped Goodyear.

Men sentenced to four months home confinement, community service, and probation.

Conviction affirmed, but Sixth Circuit requires re-sentencing (*U.S. v. Howley* (6th Cir. 2013)).
Civil & Criminal Prosecution Case Study: Victim DuPont

- Former DuPont employee took proprietary information to Korean company Kolon Industries for manufacture of Kevlar technology.
- Employee convicted and sentenced to 18 months imprisonment for theft of trade secrets and obstruction of justice.
- Civil trial against Kolon, alleging, *inter alia*, misappropriation, conspiracy to injure, civil conspiracy, and tortious interference with contractual relations ongoing.
- $920 million compensatory + $350K punitive damages against Kolon with finding of spoliation of evidence.
Contact Information

Audra A. Dial, Partner
Atlanta
404.815.6307
adial@kilpatricktownsend.com

Clay C. Wheeler, Partner
Raleigh | Winston-Salem
919.420.1717
cwheeler@kilpatricktownsend.com