Threats to Trade Secrets and Cybersecurity and Mitigation Strategies

Wes Hsu, Assistant U.S. Attorney, Section Chief, Cyber and Intellectual Property Crime Section
Steve Lee, Steve Lee & Associates, LLC
Robert Milligan, Seyfarth Shaw LLP

Introductions and Overview

Program Overview

- Cybersecurity Risks and Protection Strategies
- Legislative Solutions:
  - Economic Espionage Act
  - Theft of Trade Secrets Clarification Act and Penalty Enhancement Act
- Executive Solutions:
  - Criminal Enforcement/Options
  - Obama Administration Report – DOJ in Los Angeles
- Additional Legislation:
  - Computer Fraud and Abuse Act
  - PATSIA
  - CISPA

Cyberintrusion Detection (Mandiant)

- Median number of days a hacker was present on a network before being detected?
  - **416**
- Percentage of companies that learn they are a victim of a targeted attack from an external party (e.g. law enforcement)
  - **94%**

"The United States is the target of a ***massive, sustained cyber-espionage campaign*** that is threatening the country's economic competitiveness…."

- Washington Post discussing 2013 National Intelligence Estimate

Cybersecurity Threats

Hackers/Criminal Gangs

Political “Hacktivists”

Rogue Employees

Foreign States

Cyber Attacks

- Cybertheft ring recently accused of stealing $45 million from banks around the globe and using the loot for Rolex watches, luxury cars and other booty.
- Increasingly targeting trade secrets and confidential company information.
- McAfee Night Dragon report- attacks targeting trade secrets in the oil and gas industries.
- IBM X-Force report- Cybercriminals focusing on pinpointing valuable company data.

Foreign States/Criminal Gangs

- As laid out in the Obama administration's report on economic espionage and trade secret theft, the theft of US companies' trade secrets at the hands of foreign states has become an increasing problem.

- Criminal gangs tend to target credit card information, customer identity, etc., while state-sponsored hacking and theft tends to go after trade secrets and other information with long-term payouts.

Political “Hacktivism”

- Sentencing Commission Website
  - Protest of Aaron Swartz Prosecution and Computer Fraud and Abuse Act
- Social Media Accounts
  - Protest of Westboro Baptist Church’s Views
- Major Online Payment Providers’ Websites (Visa, Paypal, Mastercard)
  - Response to Wikileaks oppositions

Recent Employee Trade Secret Theft Prosecutions under the EEA

- Former **Motorola** engineer convicted of stealing his former employer's trade secrets.
- Former **General Motors** engineer and her husband were convicted of stealing trade secrets on hybrid- car technology from the automaker to help develop such vehicles in China.
- Former software engineer for **CME Group Inc**., the world's largest derivatives exchange, pleaded guilty to charges of downloading more than 10,000 files containing source code from his employer to support trading activities in an exchange in China.
- New Jersey federal jury convicted a former employee of **L-3 Communications Holdings Inc.'**s space and navigation division for transporting stolen property and possessing trade secrets related to precision navigation devices.

Symantec 2013 Study

- Surveyed 3,317 employees in 6 countries
- 1 in 3 employees move work files to file sharing apps
- Half of employees who left/lost their jobs kept confidential information
- 40% plan to use confidential information at new job
- Top reasons employees believe data theft acceptable:
  1. Does not harm the company
  2. Company does not strictly enforce its policies
  3. Information is not secured and generally available
  4. Employee would not receive any economic gain

Cybersecurity Risks and Protection Strategies

Risk Zones

- Network – risk examples include, but are not limited to:
  - Vendors / Partners
  - Web / Cloud
  - Failures of:
    - Access control
    - Data classification
    - Encryption
    - Patches

- User (at work, at home and everywhere else) risk examples include, but are not limited to:
  - Lost computer / device and use of unknown LANs
  - Social engineering / media “planting” by outside parties
  - Disgruntled, misguided or “turned” insider
  - Belief in the box top (e.g., anti virus reliance)

Cybersecurity Risks and Protection Strategies

Major Risk Types

- Examples include, but are not limited to:
  - False assumptions about security and kicking the cyber can down the road (compliance vs. security and form-over-substance)
  - Failure to have and then to follow security protocols / procedures / controls
  - Social media vulnerabilities / social engineering / spear phishing
  - Mobile devices – moving problems
  - Advanced persistent threats
  - Garden variety malware
  - Zero day exploits
  - Email
  - Lost / stolen media
  - Data sharing whether cloud computing or file exchange with vendors, clients, partners, etc. Encryption failures! Backup procedures?

Cybersecurity Risks and Protection Strategies

Responses and Solutions

- Prophylaxis
  - Information governance / information security
    - Procedures
    - Processes
    - Controls
    - Acceptable use
    - Who watches the watchers?
  - Info Sec Audit
    - Monitoring
    - Logging
    - Intrusion Detection
- Incident response
- Security throughline

Cybersecurity Risks and Protection Strategies

Responses and Solutions

- Employee Education
  - Training on threats, email usage, lost and stolen property, “BYOD” policies, public wifi, passwords, and foreign travel

- Employee Agreements
  - Non-disclosure agreements
  - Key employee policies such as technology and computer access policies

Cybersecurity Risks and Protection Strategies

Continuing Risks and Responsibilities

- Data Privacy/Breach Notification Requirements
  - HIPPA
  - Graham-Leach-Bliley
  - Fair Credit Reporting Act
  - Various state laws
  - FTC enforcement
  - Proposed Cyber Intelligence Sharing and Protection Act ("CISPA")
- Explosion of privacy class actions

Legislative Solutions
Overview

- Economic Espionage Act
- Theft of Trade Secrets Clarification Act
- Penalty Enhancement Act

Legislative Solutions

Economic Espionage Act

- 18 USC §1831 and §1832
- Makes the theft or misappropriation of trade secrets a federal crime
- § 1831 deals with foreign organizations and governments
- § 1832 deals with domestic misappropriation

Legislative Solutions

US v. Aleynikov

- During his last day at Goldman Sachs, computer programmer Sergey Aleynikov downloaded the code for Goldman's high frequency trading program for use at his new employer.

- Aleynikov was initially convicted in December 2010 under the Economic Espionage Act and Transportation of Stolen Property Act, but in April 2012, the Second Circuit Court of Appeals overturned Aleynikov's conviction.

- The Second Circuit based their reasoning on the fact that the trade secrets relating to the source code that Aleynikov had taken were not related to a product "produced for. . . interstate or foreign commerce," and thus, were not entitled to protection under the Economic Espionage Act.

Legislative Solutions

Theft of Trade Secrets Clarification Act

- Signed into law in late December 2012
- Strengthens the scope of the Economic Espionage Act to ensure that it addresses the theft of trade secrets *related to* a product or *service* used in interstate or foreign commerce
- Was motivated in part by decisions like the Second Circuit's opinion in *US v. Aleynikov* and the legislature's desire to expand the original Economic Espionage Act to include a trade secret "that is related to a product or service used in or intended for use in interstate or foreign commerce"
- Allows the Economic Espionage Act to protect a broader range of trade secrets

Legislative Solutions

Penalty Enhancement Act

- Signed into law on January 14, 2013
- Enhances the penalties for certain violations of the Economic Espionage Act
- Amends Section 1831 of the United States Code and provides for increased penalties for foreign and economic espionage
  - Penalties for individuals have increased from $500,000 to $5,000,000
  - Penalties for organizations have increased from $10,000,000 to either $10,000,000 or 3 times the value of the stolen trade secret

Executive Solutions

Overview

- Criminal Enforcement

- Obama Administration's Five Point Plan

Executive Solutions

Criminal Enforcement

- In December 2012, the Department of Justice released a report titled “Summary of the Major U.S. Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases.”

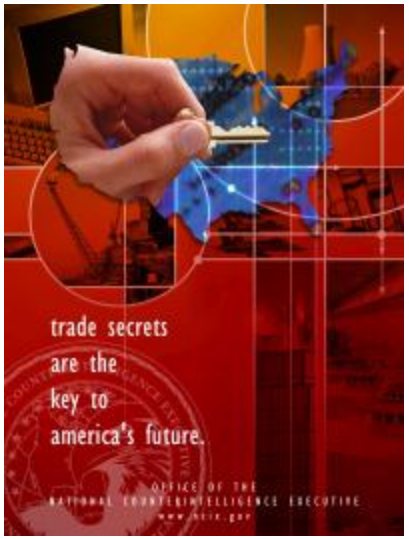
- Major trade secret prosecutions handled by the Department of Justice include:
  - *US v. Yu Xiang Dong* (theft of Ford Motor Company trade secrets to China; Eastern District of Michgan)
  - *US v. Hanjuan Jin* (theft of Motorola trade secrets to China; Northern District of Illinois)
  - *US v. Kolon* (theft of DuPont’s Kevlar fiber trade secrets to South Korea; Eastern District of Virginia)
  - *US v. Nosal* (domestic theft of former employer’s information; Northern District of California)

Executive Solutions

Obama Administration Report

- Released by the White House on February 20, 2013

- Lays out a government-wide strategy designed to reduce trade secret theft by hackers, employees, and companies



- Its five main points include:
  1) Focusing diplomatic efforts to protect trade secrets overseas
  2) Promoting voluntary best practices by private industry to protect trade secrets
  3) Enhancing domestic law enforcement operations
  4) Improving domestic legislation
  5) Promoting public awareness and stakeholder outreach

Additional Legislation
Overview

- Computer Fraud and Abuse Act ("CFAA")
  - *US v. Nosal*
  - *"Aaron's Law"*
- Protecting American Trade Secrets and Innovation Act of 2012 ("PATSIA")
- Cyber Intelligence Sharing and Protection Act ("CISPA")

US v. Nosal

Overview

David Nosal allegedly conspired with then-current employees at his former employer to illegally access and download trade secret information.

- Nosal was indicted by a federal grand jury in 2008 for, *inter alia*, violations of the CFAA and trade secret theft.
- The district court for the Northern District of California initially dismissed several CFAA counts on grounds that the employees Nosal allegedly conspired with had access to the computer systems and thus could not "exceed authorized access" under the CFAA.
- In April 2011, the Ninth Circuit Court of Appeals reversed the district court's decision, but the following year a Ninth Circuit *en banc* panel affirmed the district court's decision and reversed the prior Ninth Circuit opinion.
- The government subsequently obtained superseding indictments and charged Nosal with, *inter alia*, the remaining CFAA and trade secret theft counts.
- Nosal was found guilty on these counts on April 24, 2013.

US v. Nosal

Key Takeaways

- In analyzing whether Nosal's actions were a violation of the CFAA, the Ninth Circuit Court of Appeals focused on whether the employee originally had access to the information, not whether the employee misused the employer's confidential information in violation of usage policies. Ultimately, the Court of Appeals found that an employee's violation of his/her employer's computer usage policies was not a violation of the CFAA.

- This decision has widened the split between circuit courts regarding the proper interpretation of "unauthorized access" under the CFAA and its applicability to scenarios where employees allegedly steal company data in violation of computer usage policies or in breach of their loyalty obligations.

- It is anticipated that the case may again return to the Ninth Circuit Court of Appeal for a third decision, this time turning around Nosal's sharing of company passwords with his co-conspirators

Additional Legislation
Computer Fraud and Abuse

- After Nosal, courts and law-makers have been split over whether the CFAA should be limited to true computer hackers or if it should be extended to include employee theft of trade secret information

- Attempts to amend the CFAA include
  - The Cloud Computing Act of 2012 (Senators Amy Klobuchar (D-MN) and John Hoeven (R-ND))
  - "Aaron's Law" (Zoe Lofgren (D-CA))
  - House Judiciary Committee's March 2013 proposed amendments to §1030(a)(2)

Additional Legislation
PATSIA

- Proposed on July 17, 2012 by Senators Herb Kohl (D-WS) and Chris Coons (D-DE), but never became law
- Was intended to create one federal statute under which businesses could bring lawsuits in the federal courts, rather than requiring businesses to rely on a "patchwork" of state laws to seek redress
- Although the July 2012 version of PATSIA did not pass, President Obama's IP czar, Victoria Espinel, has asked for public comment on new federal trade secret legislation

Additional Legislation
CISPA

- Originally introduced in November 2011 by Representative Michael Rogers (R-MI) and passed the House of Representative in April 2012 but did not pass the Senate
- Was recently reintroduced and again passed the House on April 18, 2013
- Allows the government and online companies to share information regarding cyber attacks without being held liable for breach of customer privacy in order to better understand and prevent cyber attacks
- President Obama has stated that he will veto the bill if it is passed in its current form, and privacy advocates are similarly opposed to sharing information with the government

Thank You

Wes Hsu, Assistant U.S. Attorney, Section Chief, Cyber and Intellectual Property Crime Section
wesley.hsu@usdoj.gov

Steve Lee, Steve Lee & Associates, LLC
stevelee@stevelee.com

Robert Milligan, Seyfarth Shaw LLP
rmilligan@seyfarth.com

