How to Protect Your Company's Valuable Trade Secrets

Frederick Scholl, PhD, CISSP, Lipscomb University, (fred.scholl@lipscomb.edu)

&

A.J. Bahou, Esq., MSECE, Bahou Law, PLLC (aj@bahoulaw.com)

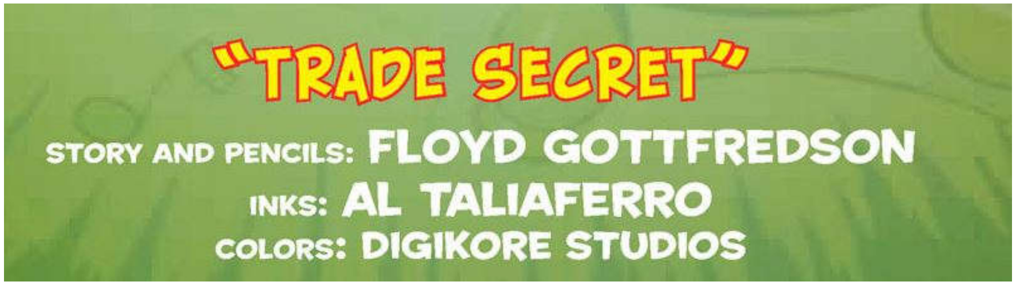
ISSA International Conference
October 2014

The views expressed herein are solely the presenter’s and do not necessarily reflect any position of Bahou Law, PLLC.

ISSA
Information Systems Security Association

Agenda

- Introduction
  - Problem to be Solved
- Trade Secrets Defined
  - State and Federal Distinctions
  - Cases
- How to Prevent Theft of Trade Secrets
  - Best Practices
- Conclusions



Risks are Growing

- US Organizations Lose nearly $300 billion per year due to Trade Secret theft or misappropriation.
- Globally, Trade Secret Theft is $0.75-$2.2T (PWC 2014)
- To protect Trade Secrets, Enterprises must engage in diligent security practices.

Unless otherwise cited, sources may be found in the article by the presenters at: Bahou, Andre and Scholl, Frederick, *Cybersecurity Protects Your Company's Valuable Trade Secrets*, ISSA Journal, vol 12, issue 3, pages 14-20 (March 2014).

Trade Secrets Defined

- Trade Secrets are a unique form of IP that can potentially last forever!
- A trade secret

  (1) is information that has commercial value,

  (2) is not easily ascertainable by others through proper means, and

  (3) is subject to reasonable efforts to maintain that information in confidence or secrecy.

Formal Definition

- Uniform Trade Secret Act (UTSA), §1(4), 1985 Amendments
  - information, including a formula, pattern, compilation, program, device, method, technique, or process, that:
    - (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by other persons who can obtain economic value from its disclosure or use, and
    - (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Misappropriation

- Generally the acquisition of trade secrets by **improper** means, misusing the trade secret, or improperly disclosing the information in violation of an obligation to keep the information secret.
  - Cybercriminals who attempt to improperly gain access to target company trade secrets
  - Employees or members of organizations who exceed their authorized access may be liable for misappropriating trade secrets.

Laws Governing Trade Secret Theft

- There are no regulations stating that you must protect your company's trade secrets!

- State Laws – Uniform Trade Secrets Acts
  - Generally - **Civil** Actions by Trade Secret Owners
  - Sometimes State Attorney General can enforce "unfair trade practices"

- Federal Laws Provide **Criminal** Prosecution
  - Economic Espionage Act, 18 U.S.C. 1832 (EEA)
  - Computer Fraud and Abuse Act, 18 U.S.C. 1030 (CFAA)
    - Can recover civil damages (in addition to state law damages)

High-Profile Trade Secrets Cases

- *U.S. v. Nosal* – theft of database records
- *U.S. v. Aleynikov* – theft of high-speed stock trading software
- *U.S. v. Howley and Roberts* – theft of tire manufacturing process and ‘know-how’
  - Please note, Government suits typically occur first, then private civil suits likely follow

U.S. v. Nosal

- Mr. David Nosal previously worked for Korn/Ferry execute search firm.
  - After Nosal left Korn/Ferry, he got some former colleagues who still worked at Korn/Ferry to start a competing executive search business.
  - Those K/F employees used their log-in credentials to gain K/F's confidential database (names, companies, and list for potential candidates).
  - Note – current employees were AUTHORIZED to access the database, but
  - The K/F Policy forbid employees from sharing info with Nosal, who was no longer working at K/F.

U.S. v. Nosal, 676 F.3d 854 (9th Cir. 2012).

U.S. v. Nosal (continued)

- U.S. Government indicted Nosal under CFAA, 18 U.S.C. 1030(a)(4) for EXCEEDING their authorized access with the intent to defraud.
  - Argued that employees violated company ‘use’ policy and
  - ‘exceeded authorized access’ by disclosing info to Nosal
- 9th Circuit Appeals Court
  - Said that violating a company’s “use” policy should not be criminal
  - Purpose of the law is punish criminal hackers, not employees who violate company’s “use” policy
  - Nosal convicted on other grounds for trade secret violations under EEA (18 U.S.C. 1832)

Goldman and Aleynikov Cases

- Mr. Sergey Aleynikov was VP at Goldman Sachs and managed group that developed source code for Goldman's high-frequency trading (HFT) system.
  - Goldman policies required employees to:
    - Keep software and proprietary info in strict confidence
    - No take any trade secrets once employment ended
  - Aleynikov accepted job offer with Teza as EVP and 3 times his salary at Goldman
    - New job was to develop HFT system for Teza within 6 months
    - Aleynikov uploaded Goldman's HFT source code to cloud server, downloaded at home, and took to Teza on flash drive.

U.S. v. Aleynikov, 676 F.3d 71, 73 (2nd Cir. 2012).

Aleynikov (continued)

- U.S. Government charged Aleynikov with stealing trade secrets under Economic Espionage Act 1832(a).
  - District Court dismissed the count on “unauthorized” access under the CFAA, 18 U.S.C. 1030, because he was authorized.

- Second Circuit Appeals Court
  - Second Circuit held that the Goldman source code that Mr. Aleynikov took was not a product “produced for or placed in interstate or foreign commerce” under that statute. Therefore, Mr. Aleynikov’s actions did not violate the EEA.

Aleynikov (continued)

- The Second Circuit stated that
  - the source code was not "produced for" or "placed in" interstate or foreign commerce.
  - Goldman gained significant value from keeping the source code and the HFT system as a trade secret.
  - Because the Goldman high-frequency trading system source code was not placed in commerce, Mr. Aleynikov's theft of the source code was not in violation of the EEA.
  - Similarly, the Goldman HFT system source code was not produced for interstate or foreign commerce because Goldman had no intention of selling its HFT system or licensing it to anyone.
  - Mr. Aleynikov's conduct was in breach of his confidentiality obligations to Goldman, and his dishonest actions should result in civil liability but not **criminal** liability under the EEA.

Goodyear Tire Case

- The Goodyear tire case is an example of an outsider attack resulting in the theft of trade secrets.
  - This case involves Goodyear, a Goodyear equipment vendor Wyko, a Goodyear competitor HaoHua, and Wyko engineers Clark Roberts and Sean Howley.
    - Goodyear manufactures tires for large earthmoving equipment at its Topeka, Kansas plant.
    - Wyko is a supplier of tire manufacturing equipment to Goodyear, but Wyko does not supply equipment needed to build very large tires.
    - HaoHua had contracted with Wyko to build just this type of equipment, but Wyko did not have the know-how to do so.

U.S. v. Howley, 707 F.3d 575 (6th Cir. 2013).

Goodyear Case (continued)

- In response to a routine equipment service request by Goodyear to Wyko, Wyko sent two of the engineers involved with this project (Roberts and Howley) to the Topeka factory.

- They took pictures of the Goodyear large tire manufacturing equipment and emailed back to Wyko engineers working on the HaoHua project.

- In this case, the email was flagged by an internal Wyko IT manager and sent back to Goodyear.

- Mr. Roberts and Mr. Howley were subsequently convicted of trade secret theft; the decision was upheld by the Sixth Circuit in February 2013.

Best Practices

- Future of Security: “More security will be done by attorneys and policy people because we are losing control of tech” (Schneier, 2012)
- Awareness
- Minimize legal vulnerabilities
- Manage third party risks
- Data Loss Prevention
- Out of the box thinking

Awareness and Beyond

- Urgency
- Create a team
- Vision and strategy
- Communicate = “awareness training”
- Empower action
- Short term wins
- Consolidate
- Anchor in culture

John Kotter,
Leading Change, 2012

Minimize legal vulnerabilities

- Non-disclosure agreements
- Employment agreements and termination policies
- Background checks
- Incident response process
- Data classification and protection

Sharing: Manage Third Party Risks

- Country by country
- Company reputational analysis
- Standards for guidance
  - ISO 27036
  - PCI 3.0
  - Office of the Comptroller of the Currency (2013)

Data Loss Prevention

- Compliance based tools
- Asset protection tools
- Secure sharing of content

Out of the Box Thinking

- Deception
- Behavioral monitoring
- Meer Kat security

More Information

- Internet Sources
  - www.pacerpro.com
  - www.tsi.brooklaw.edu

- Other Sources
  - Sources may be found in the article by the presenters at: Bahou, Andre and Scholl, Frederick, *Cybersecurity Protects Your Company's Valuable Trade Secrets*, ISSA Journal, vol. 12, issue 3, pages 14-20 (March 2014).
  - http://www.issa.org/?page=ISSAJournal

Conclusions

- The Challenge to Protect Trade Secrets is Growing
- Some New Exfiltration Paths for Trade Secrets are:
  - Cloud, Social Media, BYOD, APT
- Security Programs Must Respond Rapidly to Changing Threats
  - Consider Automating Incident Response
- Work with business leaders to develop strong Trade Secret Protection

Questions?

A.J. Bahou, Esq., MSECE

Bahou Law, PLLC

(aj@bahoulaw.com)

&

Frederick Scholl, PhD, CISSP

Lipscomb University

(fred.scholl@lipscomb.edu)