SEYFARTH SHAW

Balancing Creativity With Exclusivity

How Companies Encourage Innovation While Protecting Intellectual Property

Eric Barton, Seyfarth Shaw LLP

Agenda

01 Effect of Increased Mobility of Corporate Information On Trade Secret Protections

02 Threat to Trade Secrets from Cybersecurity Breaches and Foreign Nationals

03 Effect of Technological Advances On Professional Ethics Requirements for Lawyers

04 Conclusion

SEYFARTH SHAW

Increased Mobility of Corporate Information May Compromise Confidential Information, Including Trade Secrets

Internal Threats to Corporate Confidential Information

- Increased Risk of Misappropriation
- Inadvertent declassification of corporate information as trade secrets
  - Classification as a trade secret requires information to be the ***subject of efforts that are reasonable under the circumstances*** to maintain its secrecy
  - If no trade secret protection, then the employer is often limited to seeking contractual relief

Everyday Corporate Practices Can Undermine Trade Secret Protections

- Courts have found information as not eligible for trade secret protections based on what some consider normal, innocent, and sometimes even necessary business practices.
  - Information not sent through secured internal email by employees without being marked confidential - *B & F Systems, Inc. v. LeBlanc* (M.D. Ga. Sept. 14, 2011)
  - No prohibition on moving information between various drives on plaintiff's computers and allowing remote access - *HCC Ins. Holdings, Inc. v. Flowers* (N.D. Ga. 2017)
- Emerging trend - Courts will require claimants to show more to establish corporate information was subject to reasonable efforts to maintain the secrecy of trade secrets
  - *E.g.,* Decreased reliance on cloud based storage, remote access, increased use of internal servers and consistently labeling information as confidential

SEYFARTH SHAW

The Unexpected Threat to Trade Secrets from Cybersecurity Breaches and Foreign Nationals

External Threats to Corporate Confidential Information

- In the News – Countless Cyber Security Breaches
- Cyber threats can threaten the trade secret eligibility for company information
  - "Once a trade secret is posted on the Internet, it is effectively part of the public domain, impossible to retrieve. . . . [T]he party who merely down loads Internet information cannot be liable for misappropriation because there is no misconduct involved in interacting with the Internet." *Religious Tech. Ctr. v. Lerma* (E.D. Va. 1995).
  - Potential Shift in Law – What used to constitute "reasonable measures" to maintain secrecy may no longer be reasonable as cyber threats become more universal and apparent

National Security Implications

- Adverse governments and government-affiliated competitors target information
- Convictions under the Economic Espionage Act
  - Between January 2009 and 2013, the United States issued approximately 20 indictments for violations of the Economic Espionage Act
  - Most convictions involved active collection of trade secrets by current employees

SEYFARTH SHAW

Technological Advances In Data Sharing and Storage Have Precipitated More Stringent Professional Ethics Requirements for Lawyers

All Lawyers Have Duty to Prevent Disclosure of Client Information

- Attorneys must “take reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.” (ABA Model Rule of Professional Conduct 1.6(c)).
- ABA Formal Opinion 477R
  - Lawyers must make reasonable efforts to ensure that communications with their clients are secure and not subject to inadvertent or unauthorized cybersecurity breaches in order to meet their obligations to maintain the confidentiality of a client’s information in Rule 1.6

Failure to Enact Modern Protections Against Cyber Threats Can Have Serious Consequences

- Lawyers and/or law firms often targeted because they obtain, store and use highly sensitive information about their clients while at times utilizing safeguards to shield that information that may be inferior to those deployed by the client.
- In 2016, several prominent law firms were the subject of coordinated attacks to identify material non-public information relating to pending but unannounced mergers.
- Attorneys need to be fully aware of the technological vulnerabilities created by how a law firm chooses to handle and store client information

SEYFARTH SHAW

Conclusion

Companies May Need to Make Sacrifices at the Expense of Mobility to Protect its Trade Secrets

- While balancing a company's interest in information mobility versus security may not be easy, it is a balancing act that needs to be prioritized and deeply scrutinized in order ensure that a company is not left out to dry when its most proprietary information is at risk.

SEYFARTH SHAW

Thank You