LANDO & ANASTASI

Trade Secret Reasonable Measures: Leveraging Cybersecurity Standards

IPO Trade Secret Committee

July 7, 2020

Peter C. Lando & Dmitry Milikovsky

Trade Secret Misappropriation

- Major economic impact:
  - Estimated impact of trade secret theft in the US to be up to $600B per year (PwC and the Center for Responsible Enterprise and Trade, 2014, & The Commission On The Theft of American Intellectual Property, 2018).
  - EU: €6B direct and €54B indirect in 2018 (PwC, “Study on the “Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber”).

    https://www.pwc.com/it/it/publications/docs/study-on-the-scale-and-Impact.pdf

Data and Information Risks

- Almost all corporate data is now in electronic form.
  - Increased risk of misappropriation due to increased access.
- Access creates continuous and ongoing
- Increasing third-party collaboration increases complexity of tracking and maintaining access controls.

Legal Standards

- Legal and equitable remedies for trade secret misappropriation requires the trade secret owner to take “reasonable steps” or “reasonable efforts” to maintain the confidentiality of the trade secrets.
- Information Security Standards currently utilized provide:
  - Compliance with Data Breach Safe Harbors
  - Obtain & maintain data breach insurance
  - Privacy compliance

International Organization Standardization (ISO) 27000- series standards

- Several states allow for companies to be protected from data breach liability under the state law that creates incentives and momentum to implement the standards.
  - e.g. New York, Ohio

- ISO 27000-1 often implemented by IT and information security groups of an organization to satisfy multiple constituencies: data security organizations, data privacy compliance (CIPO), and contractual compliance.

What is ISO 27000-1?

- A set of requirements for implementing and following information security procedures.
  - The specific procedures to comply with the requirements are to be determined by company.
- Procedures subject to audit and certification by an independent third party for adherence to the procedures and reasonableness.

ISO 27000-1 Specific Requirements (examples)

1. Use of encryption for important data.
2. Training of new employees and continuous training for existing employees.
3. Continuous monitoring of activity and potential threats.
4. Security breach response and remediation.
5. Contract management & use of NDAs.
6. Measures to protect company and third-party intellectual property.
7. Requires breach response and remediation.

Protection of IP: Suggested approaches (Reasonable Measures)

- Use of non-disclosure and confidentiality agreement, A.13.4 & contractual terms to return all company information for departing employees, A.7.3.1
    - *Agilent Tech., Inc.* v. *Kirkland et al.*, 2010 Del.
- Limiting access to different types of information based upon employee and consultant roles and responsibility, A.9.1.2.
    - *Aetna, Inc.* v. *Flugel*, 2008 Conn.

Protection of IP: Suggested approaches (Reasonable Measures)

- Requires that the cybersecurity processes be monitored for compliance and reviewed regularly for improvement.
  - *Yellowfin Yachts, Inc.* v. *Barker Boatworks, LLC,* No. 17-11176 (11th Circuit 2018).
- Failure to follow policies is evidence of failing to take reasonable measures.

Value in engaging your company's ISO 27000-1 compliance process development

- Contribute to proper compliance on legal issues, e.g. NDA legal terms and departing employee communication.
  - Understand how this information is tracked and maintained.
- Access to any audit and communication to address potential risks of trade secret misappropriation.
- Notification regarding any data breach or intrusion to be able to deploy legal tools to protect trade secrets.

Thank You

Peter C. Lando

plando@lalaw.com

Dmitry Milikovsky

dmitrymilikovsky@gmail.com