BAKER & McKENZIE

Corporate Espionage and Global Security: Protecting Your Business Interests

Chicago, Illinois
February 25, 2010

Brian L. Whisler - Partner
Washington, DC

Introduction

- Piracy in Corporate Waters
- Scope of the Problem
- Threat Assessment
- Current Trends
- Counterintelligence
- Risk Management Strategies

White Collar Piracy

- Gordon Gecko
- Espionage v. Competitive Intelligence
- From Theft to Sabotage
- Cost-benefit Analysis
- Trends

Scope of the Problem

- Magnitude of the problem – theft of trade secrets exceeded $1 trillion in 2008 and continues to escalate;
- Over 40% of U.S. businesses have reported intellectual property losses;
- Corporate spies' preferred information types: R&D, financial, manufacturing processes, customer data;
- From "street crime" to global, sophisticated threat.

Threat Assessment

- Insider threats (predominant): Bribery, social engineering, exploiting privileges, disgruntled employee.
- External threats: foreign countries, individual hackers, dumpster divers.
- High Risk Industries: High technology sector, energy, military.
- Vulnerabilities: High volume of off-shore outsourcing and foreign engineering talent imported into companies and research institutions.

Current Trends

- Starwood v. Hilton (2009) - Complaint alleging that 2 former Starwood execs looted >100k Starwood computer files.

- U.S. v. Chung (2009) – Boeing employee convicted at trial for passing trade secrets to Chinese government for 30 years. Co-defendant convicted and jailed for 24 years; Chung, 74 years old, received 15 years in prison.

- US v. Zhu (2009) – Indictment alleging Chinese national employed as engineer at US environmental company stole software from his employer and sold modified version to Chinese government.

Current Trends (continued)

- US v. Lee (2009) – Former technical director of paint and coating company quit 2 weeks after return from business trip to China; discovered downloaded trade secrets, deleted files, one way ticket from Chicago to Shanghai.

- Vistakon v. Bausch & Lomb (2009) – Subsidiary of J&J alleges that B&L misappropriated trade secrets in an effort to recruit sales force to bring new contact lens product to market quickly.

Present Threat

"Kneber Bot" - Largest and most sophisticated cyber attack discovered to date targeting energy, health, technology sectors, educational institutions, federal, state and local government agencies.

- Discovered in January 2010, Eastern European criminal organization began operations in 2008 through at least 20 command and control servers worldwide, acquiring proprietary data from over 2500 companies (374 U.S. companies) in196 countries impacting over 7500 systems world wide.

Counterintelligence

- Moving from Reactive to Strategic Approach
- Identifying Business Risk
- Corporate Collaboration with FBI

Risk Management

- Know your Employees, Business Partners, Countries of Operation
- Conduct Due Diligence
- Identify Red Flags
- Share Information with Government Authorities
- Design a Trade Secrets Protection Plan

Conclusion

- A weakened economy, reduced profits, cut-throat global competition, massive layoffs, and general financial distress create a perfect storm of factors contributing to a corporate environment ripe for espionage by opportunistic employees and competitors.

- Global political climate equally ripe for espionage by nation states.

- Recent cases demonstrate ineffectiveness of traditional security approaches.

- Economic terrorism represents a clear and present danger.

Questions?

Brian L. Whisler
Partner
Baker & McKenzie, LLP
815 Connecticut Avenue, Northwest
Washington, D.C. 20006
202/452-7019
Brian.Whisler@bakermckenzie.com