Trade Secret Protection in China

Legal Developments and Best Practices

Andrew Baluch

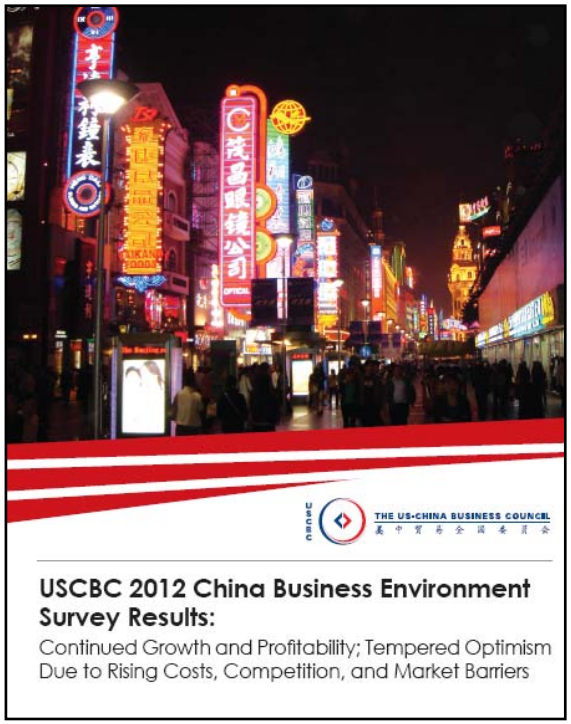
US-China Business Council
April 18, 2013

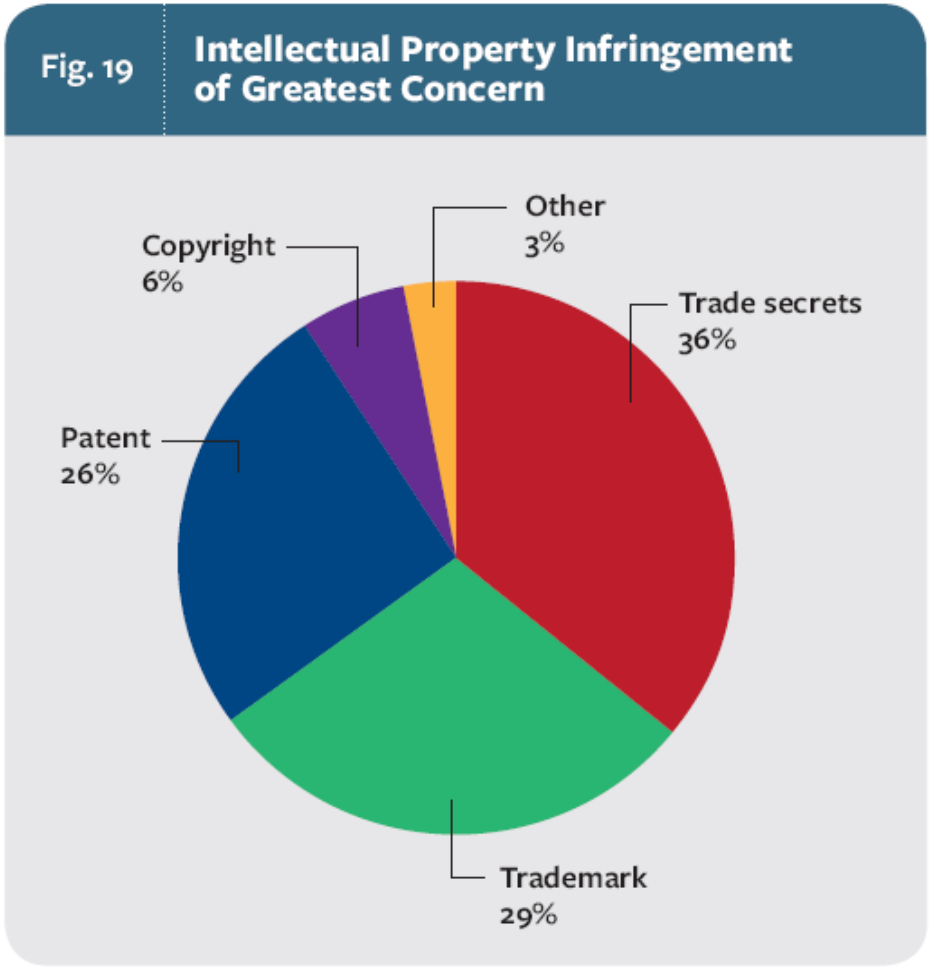
FOLEY
FOLEY & LARDNER LLP

Overview

- Recent Statistics
- Legal Framework
- Protection Strategies and Best Practices

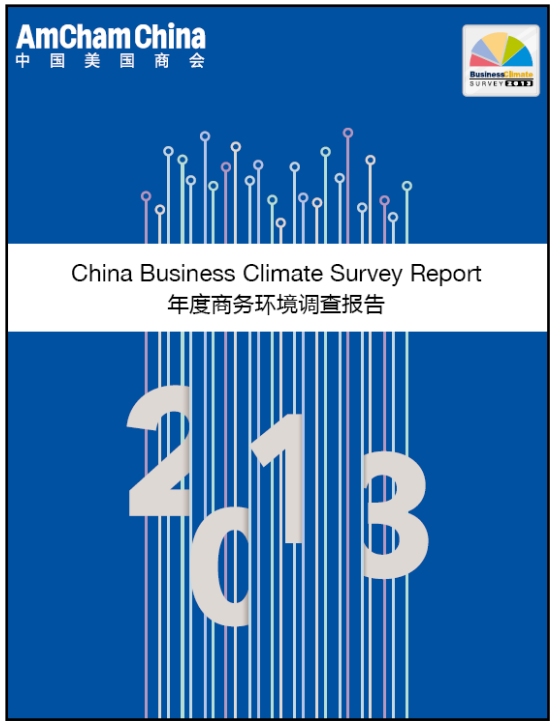
Trade Secret Theft: A Growing Problem





https://www.uschina.org/info/members-survey/2012/pdfs/uscbc-2012-member-survey-results.pdf

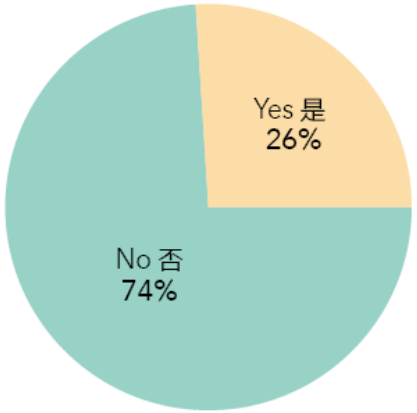
Trade Secret Theft: A Growing Problem



Over One in Four Report Data Theft
近三成企业表示遭受过数据遗失

Q Have proprietary data or trade secrets from your China operations been breached or stolen?

运营数据或贸易保密信息在中国是否出现过破坏或遗失的现象？



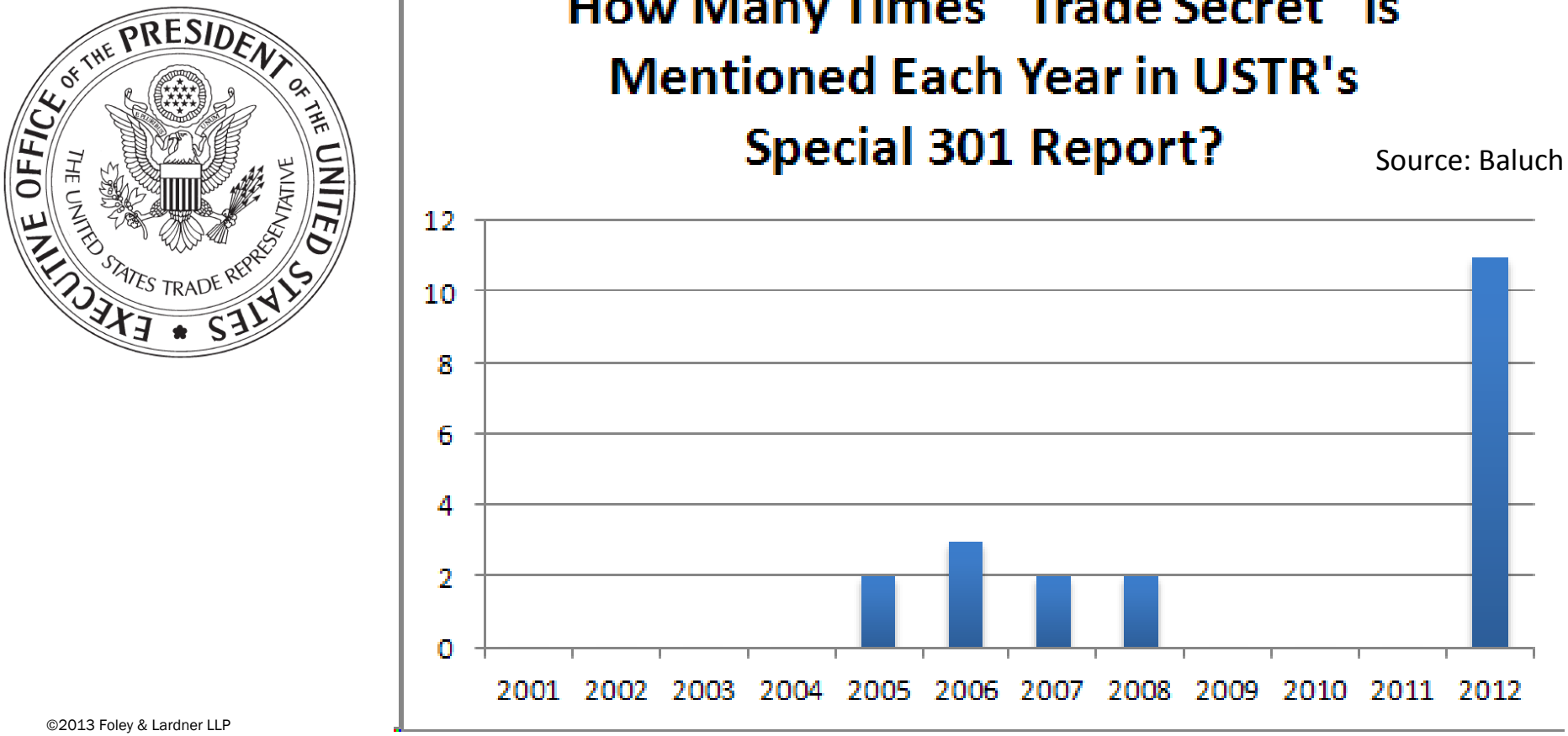
The concerns over data security are not just theoretical. Over a quarter of respondents say they have experienced the breach or theft of data and/or trade secrets from their China operations. This poses a substantial obstacle for businesses in China, especially when considered alongside the concerns over IPR enforcement and de facto technology transfer requirements.

对数据安全的担心并非仅存在于理论上。超过 1/4 的受访者表示他们在华运营的数据和／或贸易保密信息曾被破坏或窃取。这对企业在华运营造成了严重的阻碍，特别是再加上对知识产权执法和技术转让的事实要求的担心。

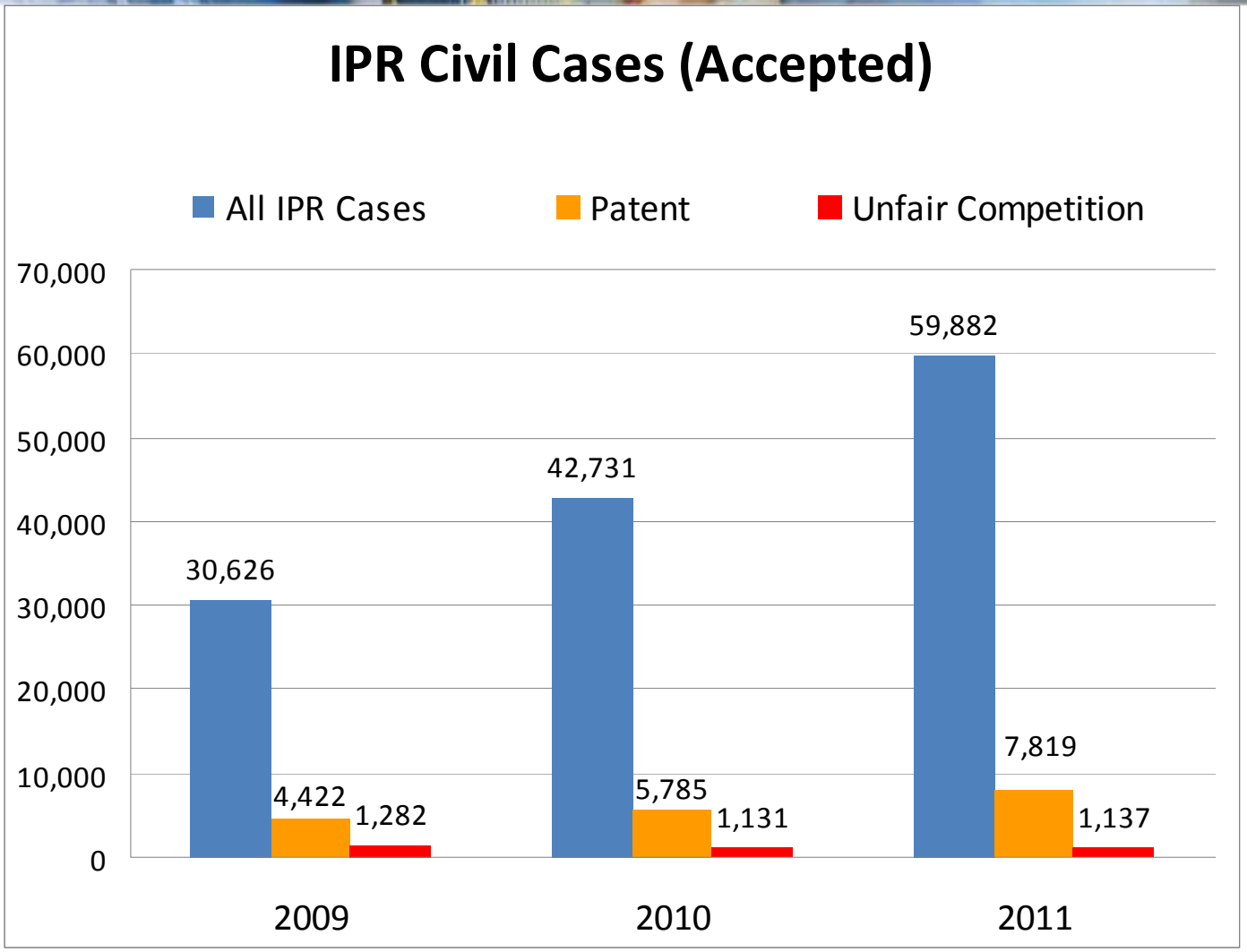
http://web.resource.amchamchina.org/cmsfile/2013/03/29/0640e5a7e0c8f86ff4a380150357bbef.pdf

Trade Secret Theft: A Growing Problem

- US Trade Representative's Special 301 Report



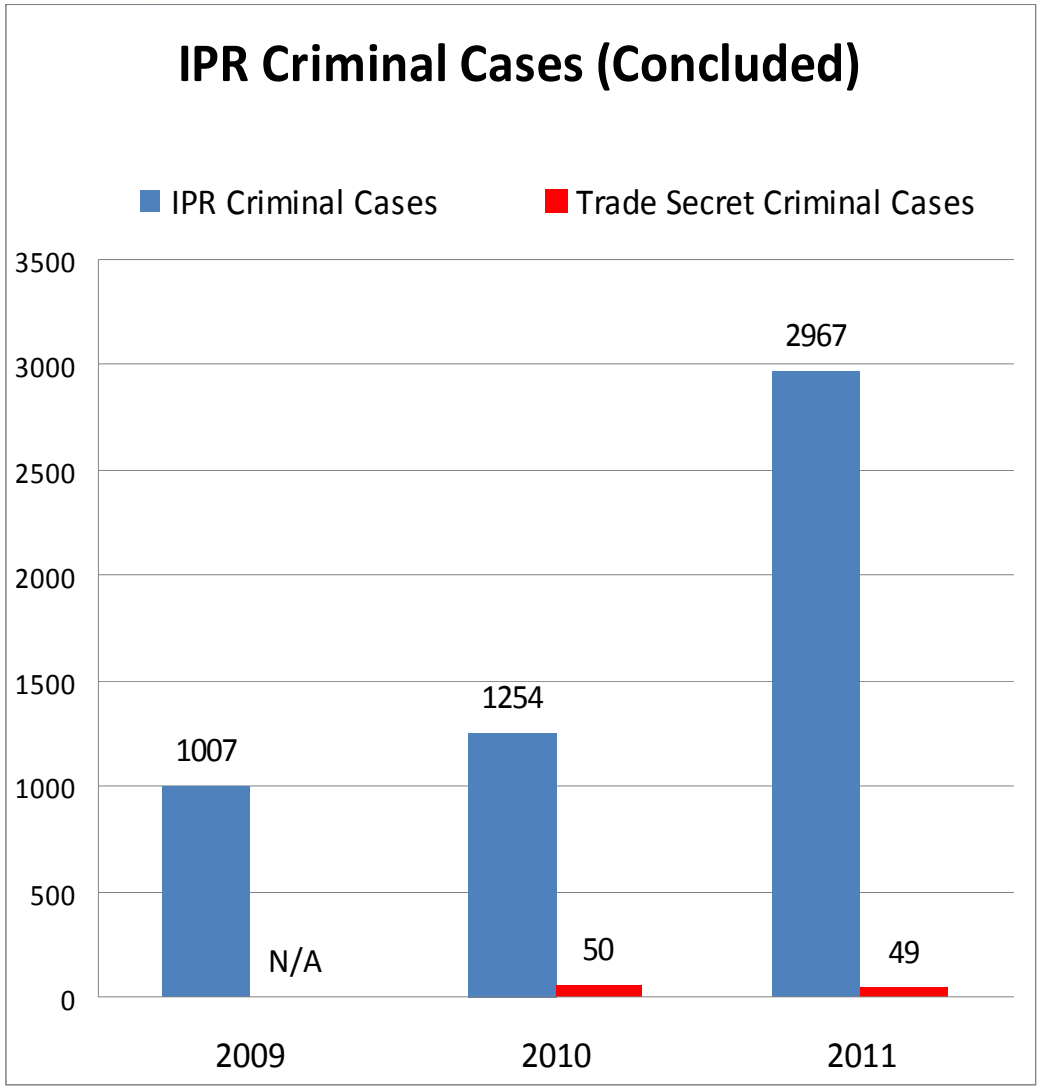
China Trade Secret Statistics



<u>Unfair competition</u> includes false advertising, false designation of origin, business bribery, antitrust liabilities, and **trade secret misappropriation**.

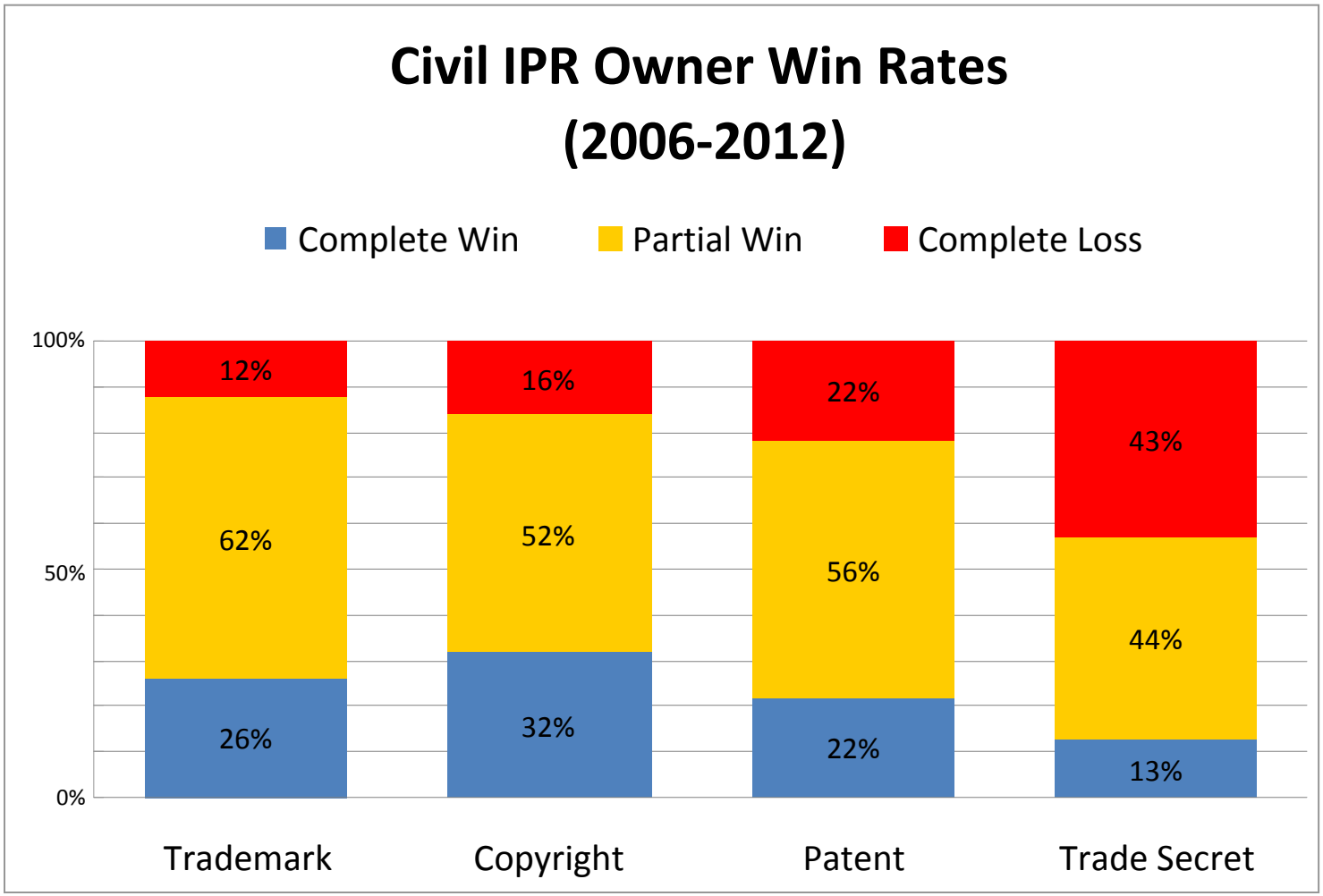
Source: PRC SPC

China Trade Secret Statistics



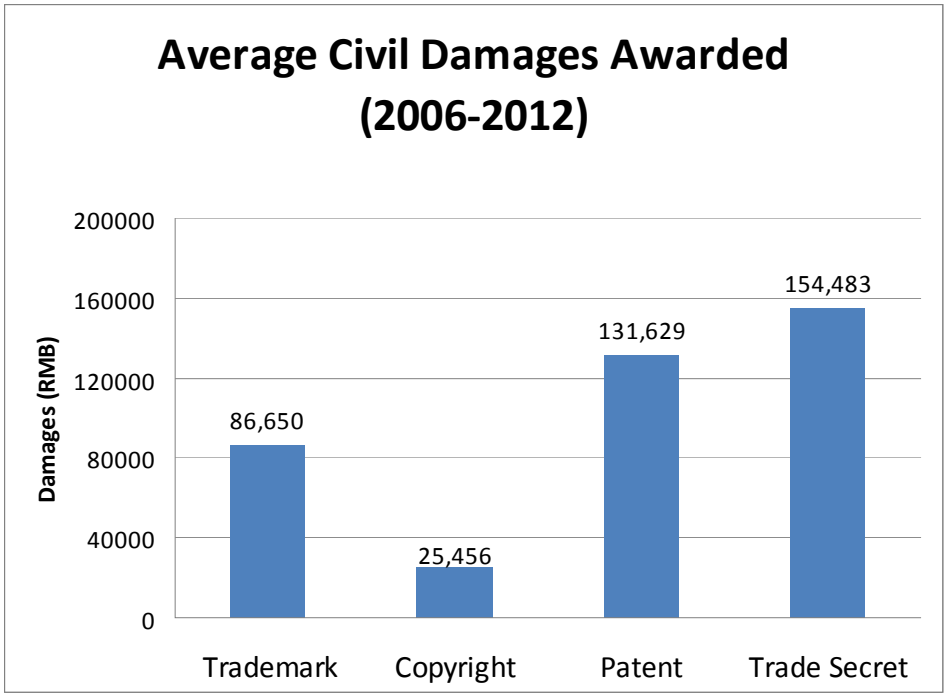
Source: PRC SPC

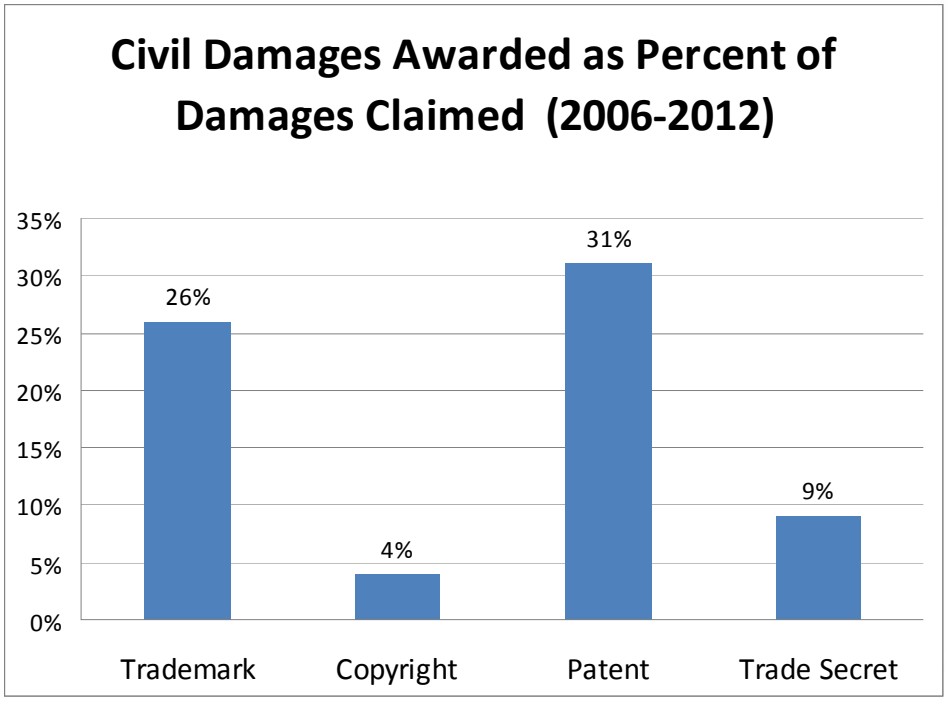
China Trade Secret Statistics



Source: CIELA

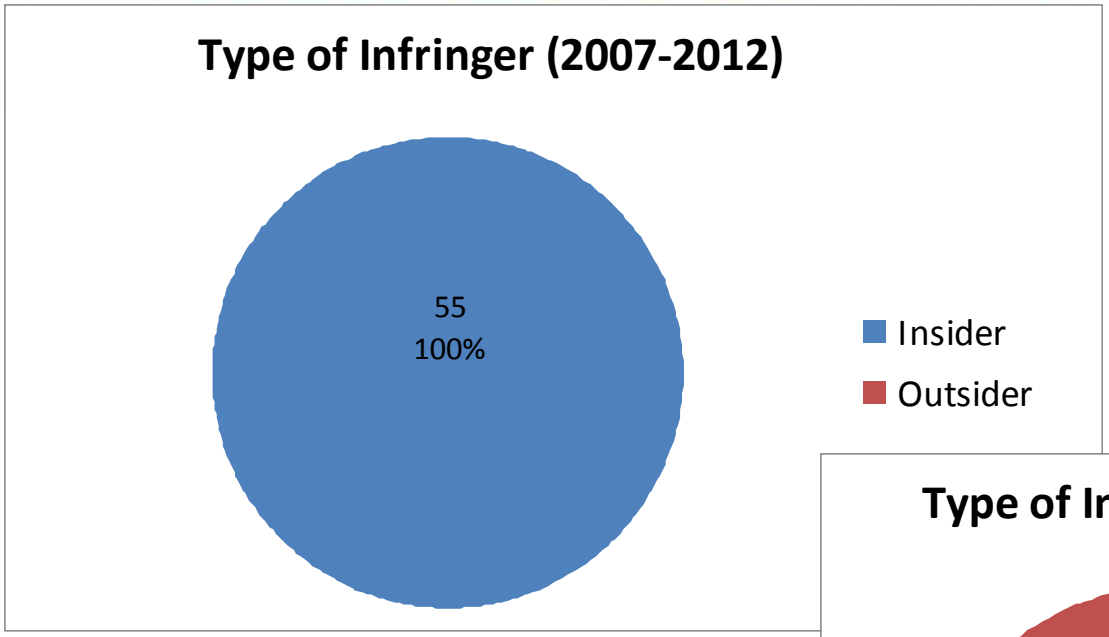
China Trade Secret Statistics



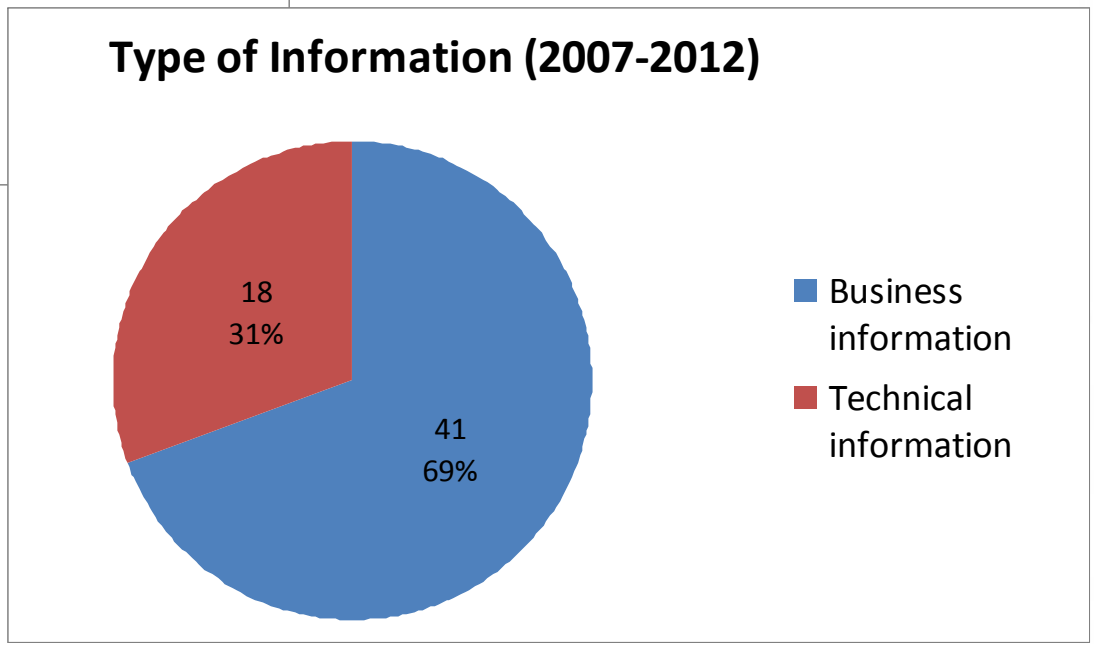


Source: CIELA

China Trade Secret Statistics



Source: Baluch



Sources of PRC Trade Secret Law

- Laws
  - Guarding State Secret Law (1988)
  - Anti-Unfair Competition Law (1993)
  - Criminal Law (1997)
  - Contract Law (1999)
  - Company Law (2005)
  - Labor Contract Law (2007)
- Regulations
  - SAIC Provisions on Prohibiting Trade Secret Misappropriation (1998)
  - SPP and MPS Regulations on Prosecution of Economic Crime (2001)
  - SASAC Interim Provisions on Trade Secret Protection in Central Administered SOEs (2010)
- Judicial Interpretations
  - SPC and SPP Interpretations on Handling Trade Secret Criminal Cases (2004)
  - SPC Interpretation on Civil Cases Involving Unfair Competition (2007)

Definition of Trade Secret

- Technical information or business information:
  - which is unknown to the public,
  - capable of bringing economic benefit to the owners and having practical utility, and
  - the owner has taken reasonable measures to keep it secret.

(Art. 10 of AUCL)

"Unknown to the Public"

- **Not** a trade secret if the information is:
  - Common sense
  - Disclosed in a publication
  - Acquired through public channels
  - Easily acquired without substantial efforts or costs.
- **Reverse engineering** is a defense.
  - Not an act of infringement if it was "obtained by dismantling, mapping or analyzing the products obtained from public channels."

(Art. 9 and 12 of SPC Interpretation)

"Reasonable Measures to Keep It Secret"

- Courts will consider whether:
  - (1) access to the classified information was limited on a "need to know" basis;
  - (2) the media of the information was locked up or other preventive measure was taken;
  - (3) classified information was marked as confidential;
  - (4) passwords or codes are used to access the information;
  - (5) a confidential agreement was entered into;
  - (6) visitors are prohibited from entering into facilities or required to maintain confidentiality;
  - (7) any other measures was adopted to ensure confidentiality.

  (Art. 11 of SPC Interpretation)

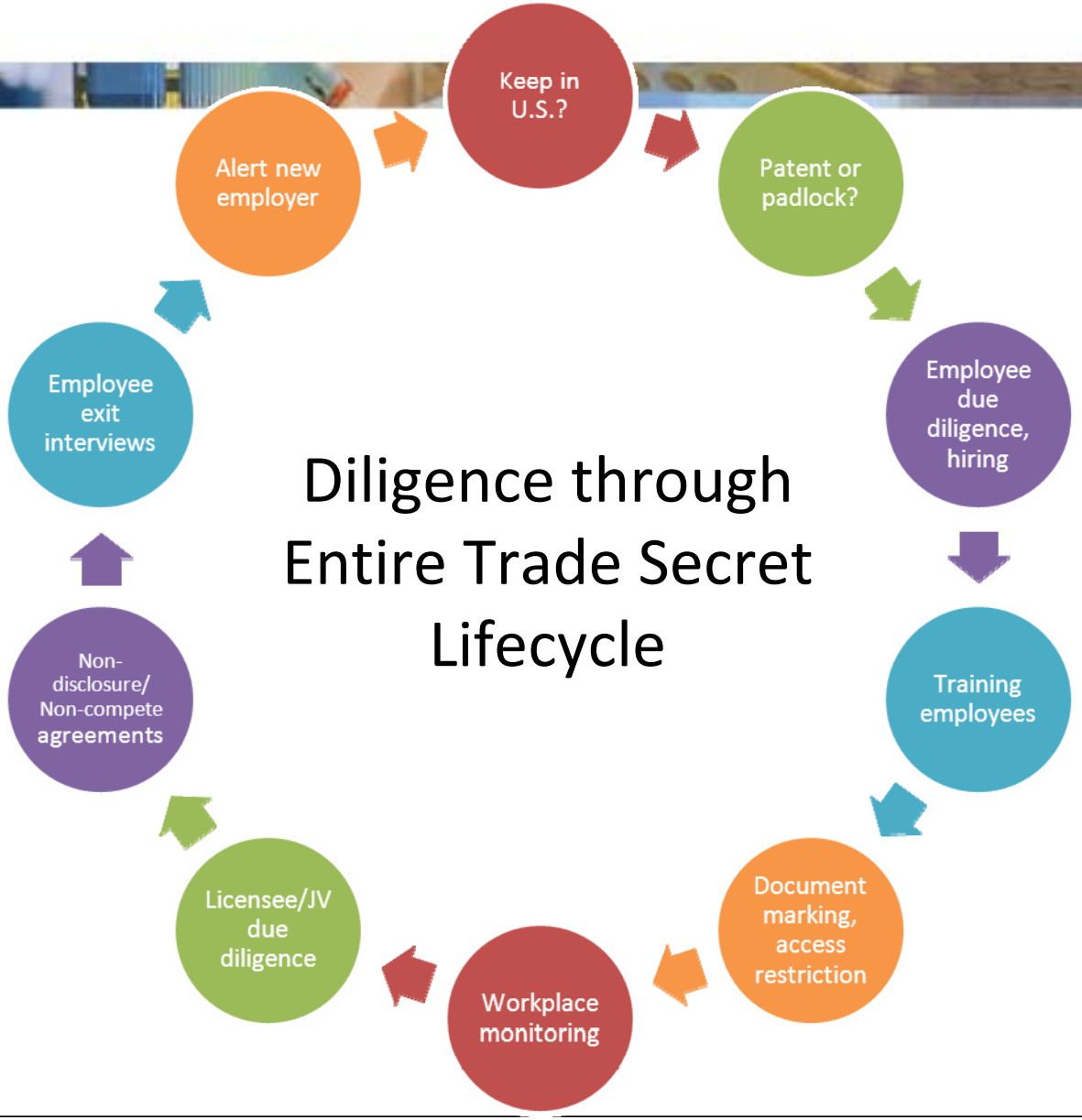
Trade Secret Enforcement Channels

	Civil Court Action	Administrative	Criminal
Enforcement Powers	•Owner can recover damages. •Preliminary and permanent injunctions. •Evidence preservation (including before suit).	•Fines (RMB 10,000-RMB 200,000). •Order infringement to stop. •Order destruction of products. •Evidence collection.	•Imprisonment and fines (up to 3 yrs prison if loss of RMB 500,000 to 2.5 million; up to 7 yrs if loss greater than RMB 2.5 million). •Treble fines if corporate entity. •Broad evidence collection.
Procedural Shortcomings	•Case acceptance by courts requires actual evidence. •No US-style civil "discovery" in China. •Emphasis on original documentary evidence; not witness testimony. •No "inevitable disclosure" doctrine.	•Case acceptance by AIC is discretionary. •Case acceptance requires some actual evidence. •AICs typically want simple cases. •Owner cannot recover damages.	•Case acceptance by PSB is discretionary, requiring "serious loss" (RMB 500,000). •Owner cannot recover damages. •Public prosecution does not include owner as party. •Private prosecution does not give owner evidence collection tools.

Trade Secret Best Practices

- FBI, The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy, http://www.fbi.gov/about-us/investigate/counterintelligence/insider_threat_brochure
- FBI, Safeguard Your Company's Trade Secret, Proprietary Information and Research, http://www.fbi.gov/about-us/investigate/counterintelligence/intellectual_property_protection
- FBI, Visitors: Risks & Mitigations, http://www.fbi.gov/about-us/investigate/counterintelligence/Risks%20-%20Mitigations%20of%20Visitors%20Brochure.pdf
- ONCIX, Foreign Spies Stealing US Economic Secrets in Cyberspace, http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf
- SEI CERT, Common Sense Guide to Mitigating Insider Threats, 4th ed., http://www.sei.cmu.edu/reports/12tr012.pdf
- CREATe, Trade Secret Theft: Managing the Growing Theft in Supply Chain, http://www.create.org/sites/default/files/CREATe_White-Paper_Trade-Secret-Theft_Final-e.pdf
- Bai & Da, Strategies for Trade Secrets Protection in China, http://scholarlycommons.law.northwestern.edu/njtip/vol9/iss7/1
- Garvey & Baluch, Patent or Padlock: Patents and Trade Secrets Form the Heart of an Effective IP Strategy, http://www.nxtbook.com/nxtbooks/advanstar/biopharm0207/index.php?startid=34
- Ong, Trade Secret Enforcement in China: Options and Obstacles, https://www.chinabusinessreview.com/members/1301/ong.html
- Dexter & Park, Protecting Trade Secrets in Knowledge-Based Industries, http://www.fbm.com/files/Publication/856a6ff2-cef7-4f26-b812-c25c6dabdfba/Presentation/PublicationAttachment/c804933e-b6d9-4180-9dc2-c2d4103f05f1/1074C1FF-0DCB-41E5-92E7-5F778F1F7AA7_document.pdf

Trade Secret Best Practices



Best Practices: Employees

- New Employees
  - Background checks
  - IP assignment to company
  - Confidentiality agreement
  - Non-compete agreement
  - Confidentiality Policy, acknowledging having read it and understand
    - Including policy against disclosing *prior* employer's trade secrets
- Departing Employees
  - Exit interview, with written acknowledgment and reaffirmation, certifying the return of all documents and company property
    - Including promise that nothing is saved on personal computer or storage devices
  - Immediately terminate all electronic and physical access
  - Notify new employer of employee's ongoing secrecy obligations

Best Practices: Potential Customers, Licensees and Partners

- Take precautions **before** the meeting
  - Background checks
  - File U.S. *Provisional* Patent Application (which does not publish)
- Take precautions **during** the meeting
  - Signed acknowledgement and description of trade secrets received
  - Execute three-way confidentiality agreements between:
    - You
    - Your partner
    - Your partner's employees
  - Liquidated damages in case of breach
- Take precautions **after** the meeting
  - Ongoing inspection rights
  - Ongoing secrecy obligation
  - File Chinese and U.S. Regular Patent Applications on any leaked technical information
    - In China, must file within 6 months (PRC Patent Law art. 24)
    - In US, must file within 1 year (35 US Code § 102(b))

Best Practices: Hiring IT Security Firms

THE WALL STREET JOURNAL.
WSJ.com

LAW JOURNAL | Updated March 31, 2013, 7:17 p.m. ET

Law Firms Tout Cybersecurity Cred

By CHRISTOPHER M. MATTHEWS

"Mike Dubose, the head of Kroll Advisory Solutions' cyber-investigations practice, says **Kroll advises its clients to hire a lawyer first and then have the lawyer hire Kroll**. While a forensics firm such as Kroll can detect malware, scour network-access logs or understand the modus operandi of a foreign hacking group, if Kroll is contracted directly by the company rather than by an outside lawyer, that work is unlikely to be protected by **attorney-client privilege**, he says."

Best Practices: Publicly Traded Companies

- **U.S. Securities and Exchange Commission (SEC)**
  Disclosure Guidance on Cybersecurity (Oct. 13, 2011)
  - "Registrants should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky."
  - "A registrant may need to disclose known or threatened cyber incidents to place the discussion of cybersecurity risks in context."
  - "If one or more cyber incidents materially affect a registrant's products, services, relationships with customers or suppliers, or competitive conditions, the registrant should provide disclosure in the registrant's 'Description of Business.'"
  - "If the incident constitutes a material nonrecognized subsequent event, the financial statements should disclose the nature of the incident and an estimate of its financial effect, or a statement that such an estimate cannot be made."

http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

United States Law Enforcement

- U.S. Department of Justice
  - Economic Espionage Act applies to conduct occurring outside of the United States if:
    - the offender is a natural person who is a **citizen** or **permanent resident alien** of the United States, or an **organization** organized under the laws of the United States or a State or political subdivision thereof; or
    - an **act in furtherance of the offense** was committed in the United States. (18 U.S.C. § 1837)
- U.S. International Trade Commission
  - Section 337 of Tariff Act applies to goods that are **imported** into the United States which contain, or were made using, a trade secret that was misappropriated outside of the United States. (19 U.S.C. § 1337; *TianRui v. ITC*, 661 F.3d 1322 (Fed. Cir. 2011))

Contact Information

Andrew Baluch
Intellectual Property Special Counsel
Foley & Lardner LLP
Shanghai, China
abaluch@foley.com

Andrew Baluch advises companies on global IP strategies, including international portfolio management, IP diligence reviews, opinions, licensing, litigation, patent reexamination, and trade secret protection. As a member of the firm's China practice, Mr. Baluch provides clients with information on the impact of the Chinese legal environment.

Mr. Baluch is a former director of international enforcement in the White House Office of the IP Enforcement Coordinator. In this role, he oversaw implementation of all international IP enforcement initiatives in the US Government's Joint Strategic Plan on IP Enforcement and coordinated U.S. Embassy personnel stationed in 17 priority countries, including China, Brazil, Russia and India. His responsibilities also included convening inter-agency teams to assist companies facing IP theft abroad and participating in all major bilateral trade dialogues with China, including the US-China Joint Commission on Commerce & Trade (JCCT) and the U.S.-China Strategic & Economic Dialogue (S&ED).

Prior to his White House appointment, he was an expert legal advisor to the under secretary and director of the U.S. Patent & Trademark Office (USPTO).

Mr. Baluch served as a law clerk to Judge Richard Linn of the U.S. Court of Appeals for the Federal Circuit and was an associate with Foley before this service.