WINSTON & STRAWN LLP

Understanding Trade Secret Laws

March 19, 2019

Today’s Webinar Presenters

Aviva Grumet-Morris

Partner
Chicago

Aviva focuses her practice on labor and employment issues, including litigation in state and federal trial and appellate courts. She has experience at all levels of litigation, from unemployment hearings to trial court litigation to appellate advocacy, and strives to provide clients with practical, timely advice in connection with all of their employment needs.

Shannon Murphy

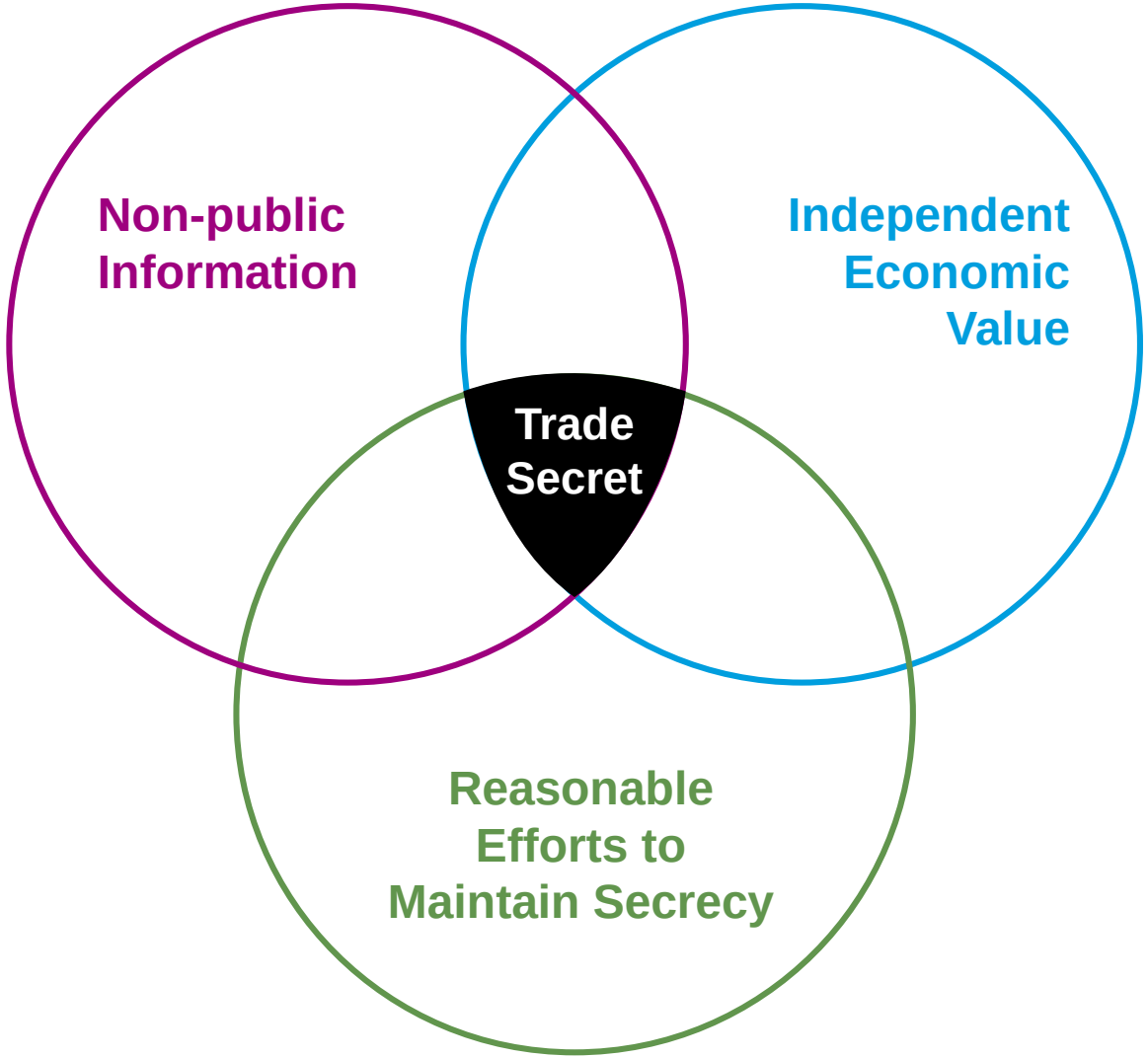
Partner
Chicago

Shannon is a litigator, investigator, and data protection attorney who deploys her computer forensic knowledge, theft of trade secret expertise, and decade of criminal justice experience to counsel and protect clients’ interests, with a focus on protecting valuable corporate data.

Trade Secret Laws

WINSTON & STRAWN LLP

What Is a Trade Secret?



Legal Remedies in the U.S.

Civil – Federal: Defend Trade Secret Act	• Injunctive relief • Actual loss, restitution, or reasonable royalty • Enhanced (trebled) damages and attorneys' fees in some cases • *Ex parte* seizure
U.S. Individual States: modeled after UTSA	• Injunctive relief • Actual loss or reasonable royalty • Enhanced (trebled) damages and attorneys' fees in some cases
Criminal – Federal: Economic Espionage Act	• Applies to individuals, organizations and companies • Includes attempting to or conspiring to steal trade secrets • *Also Computer Fraud and Abuse Act, Mail Fraud

The Significant and Growing Risk of Trade Secret Theft

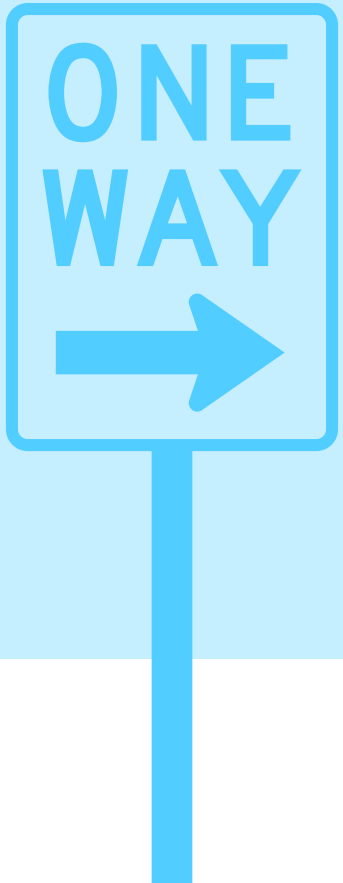
WINSTON & STRAWN LLP

Data Theft Is Becoming Inevitable

THE PAST

WHETHER

THEFT WOULD OCCUR



THE PRESENT

WHEN

THEFT WILL OCCUR &

HOW

DAMAGING WILL IT BE

Potential Threats

- **Insiders**
  - Employees
  - Contractors/temporary employees
  - Vendors
- **Partners**
  - Manufacturers
  - Vendors
  - Suppliers
  - Joint-venture partners
- **Outsiders**
  - Hackers
  - Foreign governments

REVERSE THREAT: new employees injecting trade secrets from former employer into company's systems/products

Employees Do Not Safeguard Data

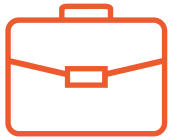
82% of respondents acknowledged that it was “very likely” that high value company assets had been breached

79% of CEOs **65%** of employees believe that the company’s assets are now in the hands of a competitor

72% of CEOs admitted to taking intellectual property from their previous employers

44% of employees do not believe it is a crime to use a competitor’s trade secrets

40% of employees plan to use at new job



Recent Developments, Challenges, and Cautionary Tales

WINSTON & STRAWN LLP

Current Trade Secret Focus: China

UNITED STATES DEPT. OF JUSTICE NOV. 1, 2018
Attorney General Announces New Initiative to Combat Chinese Economic Espionage

CORPORATE COUNSEL NOV. 9, 2018
Why Trade-Secret Theft Prosecutions vs. China are Trending: Lawyers Explain

THE WALL STREET JOURNAL SEPT. 26 2018
How China Systematically Pries Technology from U.S. Companies

REUTERS Nov. 15, 2018
Exclusive: German Prosecutors Charge Chinese-Born Engineer in Industrial Espionage Case

Bloomberg Jan. 28, 2019
U.S. Charges Huawei with Stealing Trade Secrets, Bank Fraud

THE WALL STREET JOURNAL Jan. 30, 2019
Apple Engineer Stole Material on Autonomous Vehicles, FBI Alleges

THE WALL STREET JOURNAL Feb. 14, 2019
Former Coke Scientist Accused of Stealing Trade Secrets for Chinese Venture

Current Trade Secret Focus: China

US Department of Energy Critical of China's "The Thousand Talents" award – "used to solicit and reward the theft of United States trade secrets."

- Assistant Attorney General of the National Security Division, John Demers:
- "premeditated theft" that "exemplifies the ***rob, replicate and replace*** approach to technological development."
- "China wants the fruits of America's brainpower to harvest the seeds of its desired economic dominance."

Large Settlements and Verdicts

$21.2M

Average damages award between 1990 and 2015

$919.9M

Largest damages award

> $2B

Pending case

2018: High Damage Awards and Settlements

$245M settlement in self-driving car case	$706.2M jury award in Amrock software case	$223M jury award for Dutch semiconducter maker + $1.2M for investigation costs

Courts Pushing on “Reasonable Measures” Requirement

NOT
Take Reasonable Measures

=

NOT
A Trade Secret

2009 to 2018: more than 11% of claims dismissed for lack of “reasonable measures”

Lack of Clarity Regarding Confidentiality Marking Policies

To Mark?

Viewed as reasonable measure

Puts potential thief on notice

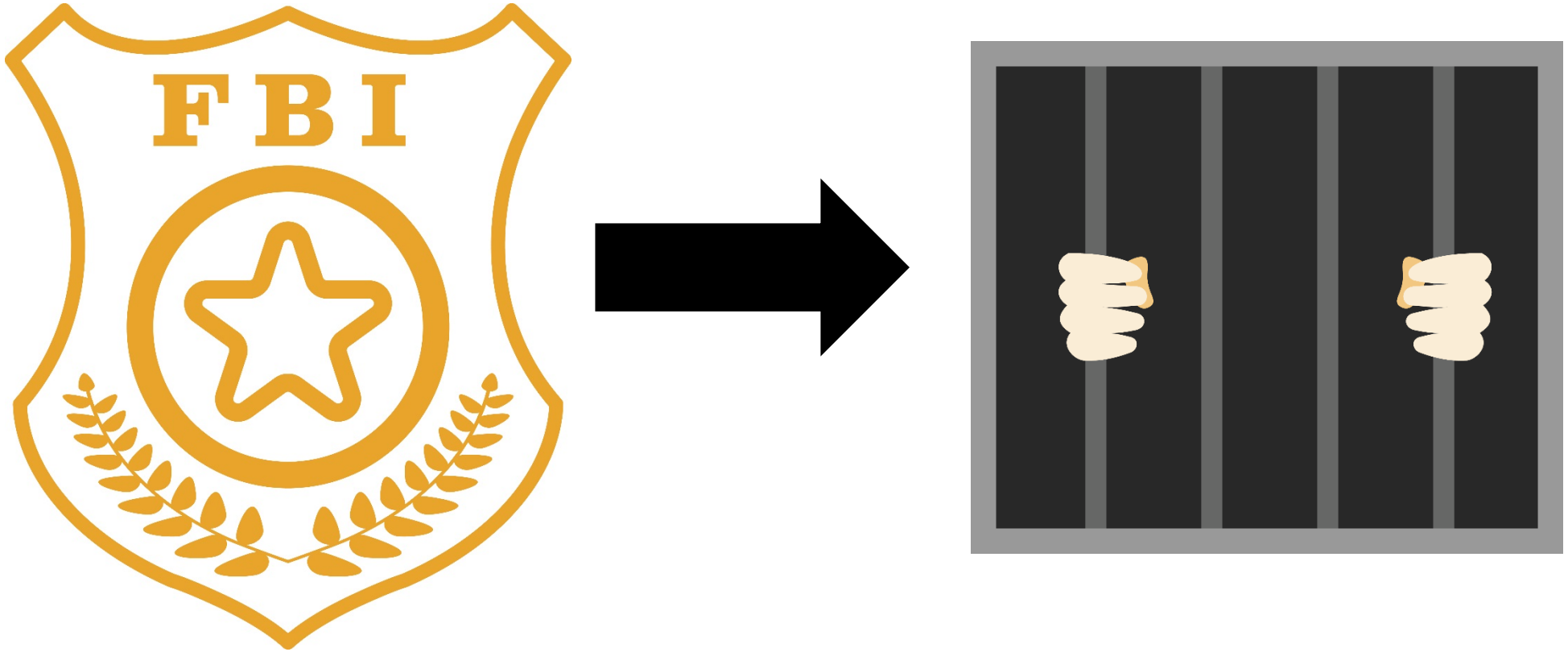
Some courts think dispositive

Or Not to Mark?

Failure to abide by policy can undermine claim

Fact-based determination

Promotion of Cooperation with Law Enforcement



Prevention Improvement Is Needed

82%	impediments to protecting trade secret
39%	lack of awareness that theft occurred
20%	lack of affirmative steps to limit access
20%	do not have HR procedures when employee terminated/resigns

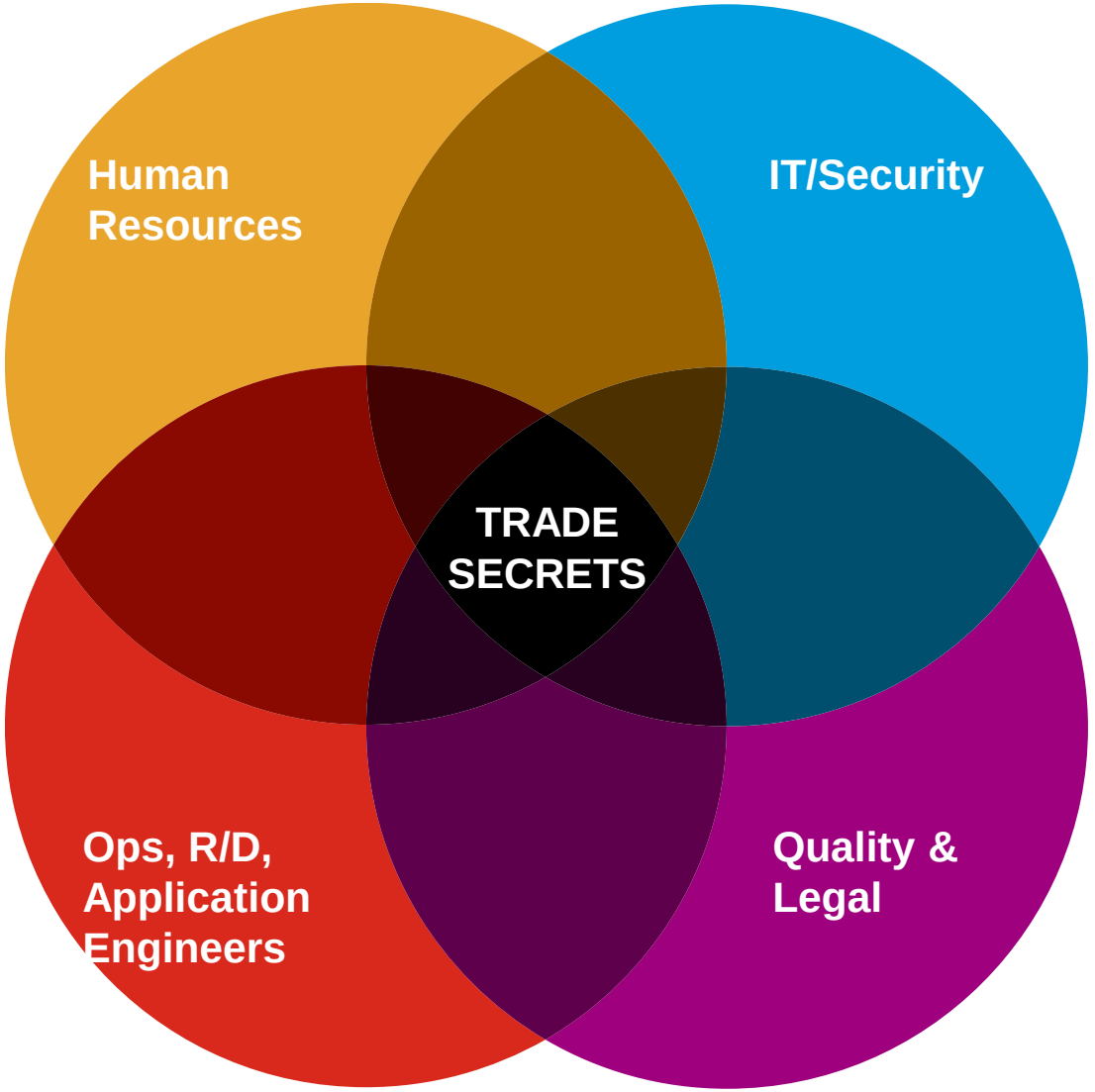
Practical Guidance for Protecting Corporate Trade Secrets

WINSTON & STRAWN LLP

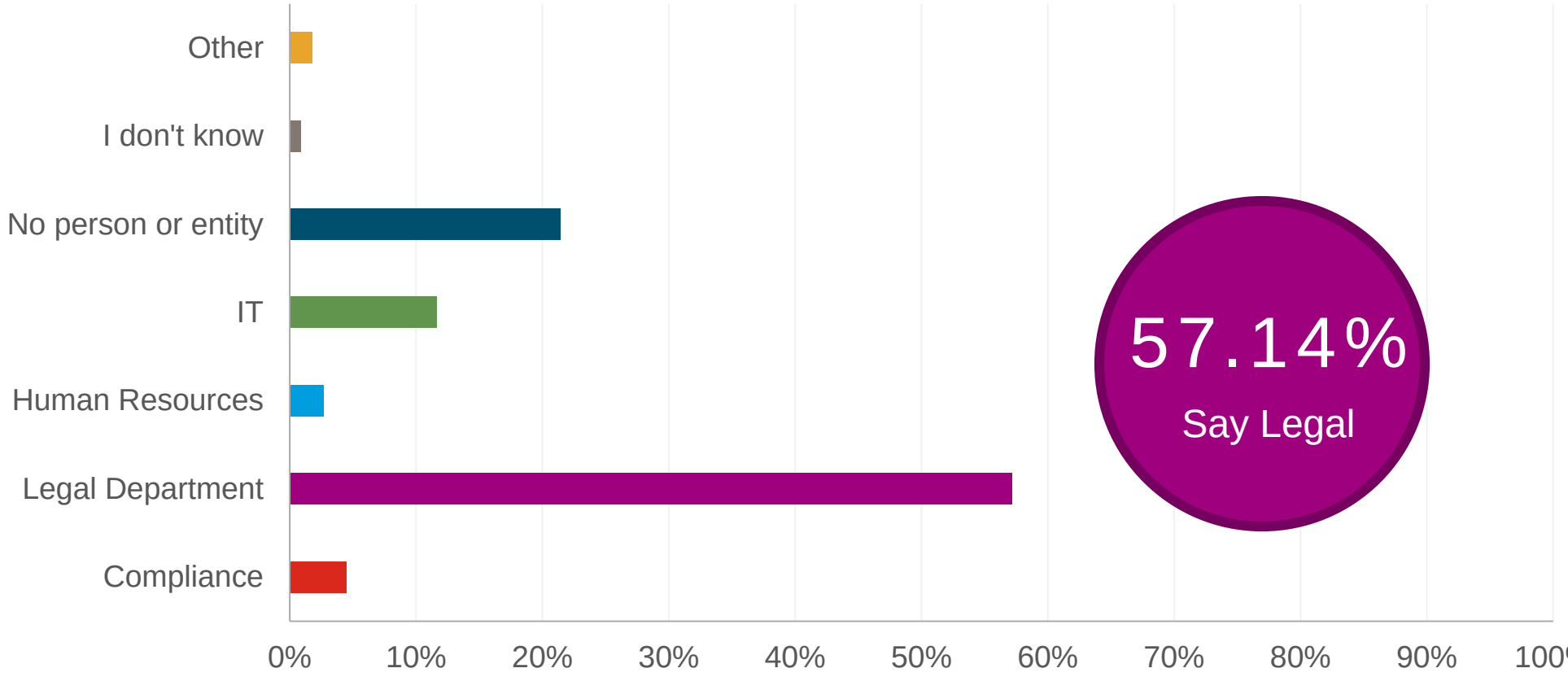
Proactive Approach to Trade Secrets

Two Goals: minimizing theft + increasing legal options

A Holistic/Cross-Functional Approach



Owners of the Trade Secrets Risk



	Compliance	Legal Department	Human Resources	IT	No person or entity	I don't know	Other
Answer Choices	4.46	57.14	2.68	11.61	21.43	0.89	1.79

1) Identify, Prioritize and Limit Access to Trade Secrets

- What are the company's trade secrets?
  - High-level, categories
  - Not need to identify all
- Where/how are they stored?
- Which are the most valuable?
  - Can prioritize by business unit or across the company

Taking "reasonable" proactive protective measures is key

*One size does not fit all

2) Consider Red Flags During Hiring

- Reference check
- Employment history
- Evaluate how employee discusses former employer during hiring
- Beware of red flags

3) Use Robust and Enforceable Agreements

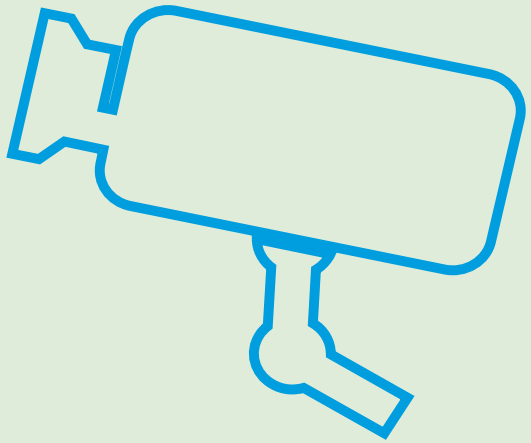
- Employee agreements:
  - Nuances of states' restrictive covenant laws
  - "Reasonable" restrictions
  - Include key stipulations to bolster enforceability
  - Whistleblower or privacy language may be required
- Third-party agreements:
  - Maintain confidentiality
  - Return/destroy data
  - Audit rights

4) Draft Precise Policies + Train Employees

- IP ownership
- Confidentiality
- Acceptable IT and email use
- Indemnification
- No expectation of privacy
- Cooperation obligation

5) Implement Ways to Catch Theft

- Download alerts
- Email attachment alerts
- Key logger
- Monitoring
- Software
  (i.e. homing beacon)
- Utilize reporting hotline



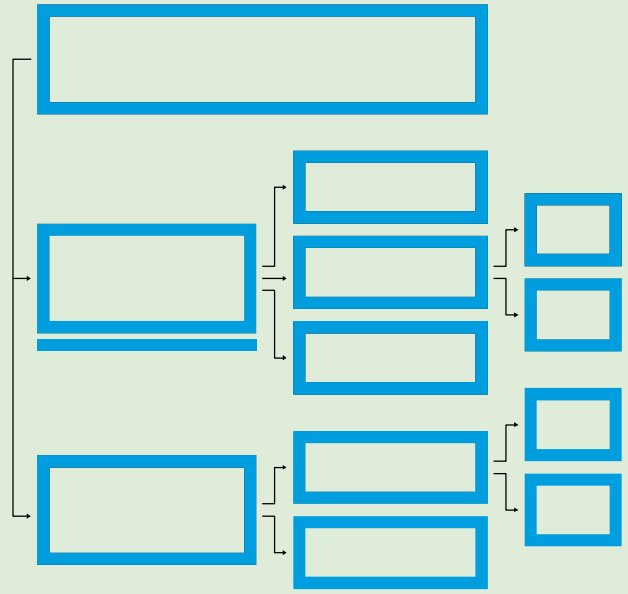
*Can and should be tailored to particular types of employees based on role, risk, or level of access

6) Have Sufficient Exit Protocols

- Terminate physical and electronic access completely and promptly
  - Consider limiting access if employee continues to work
- Conduct an exit interview
- Require the employee to re-certify obligations
- Assess risk of theft → heightened protocols

7) Establish a Response Protocol

- HR, legal, managers, IT and other key players must know specific steps to take immediately
- Should include guidance for:
  - maintaining privilege
  - document retention
  - protecting confidentiality
  - reporting results
  - clear reporting structure
  - engaging outside experts (the earlier the better!)



What To Do After Theft Occurs

WINSTON & STRAWN LLP

1) Properly and Broadly Preserve Evidence

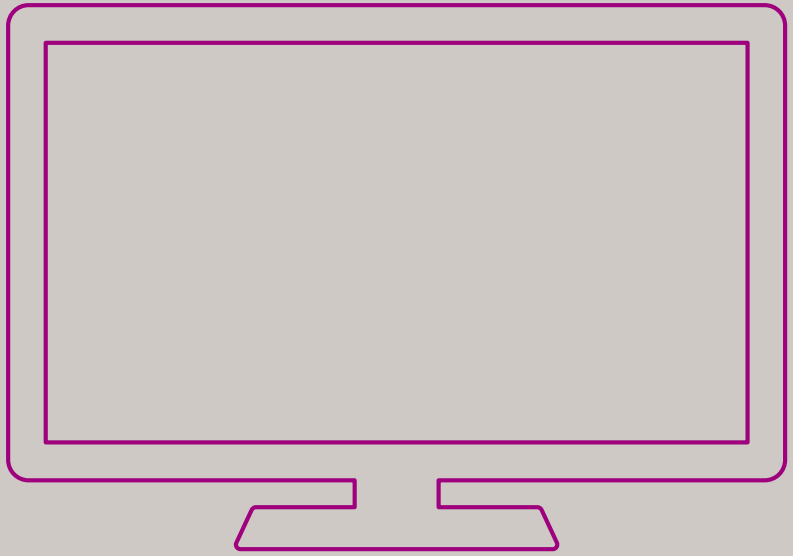
- Must promptly preserve:
  - Devices
  - Logs
  - Emails
  - Documents
  - Video
  - Online storage/apps

2) Maintain and Document Chain of Custody

- Document collect
  - Make, model, serial number
  - When collected
  - By whom
  - From whom/from where
- Store securely
- Document any change in custody

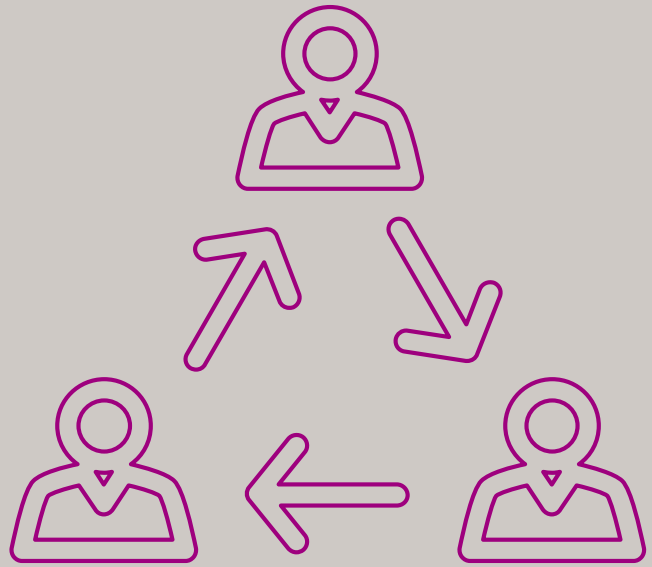
3) Image a Device Before Any Review

- Do not take any steps to review a device until a forensic copy has been made
- Train “well-intentioned” IT personnel
- Even turning on/off a computer can lose or change important data



4) Consider Referral to Law Enforcement

- Broader investigative tools (e.g. subpoenas, search warrants, wire taps, compelled testimony)
- Costs of cooperating with law enforcement recoverable as restitution
- Charges/conviction have deterrent effect
- Act as good corporate citizen
- BUT – “lion out of the cage”



5) Maintain Privilege

- Nuanced Privilege Issues
  - Take investigative steps "at direction of counsel"
  - Mark documents, notes, and memoranda
  - Give Upjohn warnings
  - Take care disclosing information to government agencies

Prevent Stolen Secrets from Entering Your Company

1. Train interviewers to avoid perception of hiring for prior access

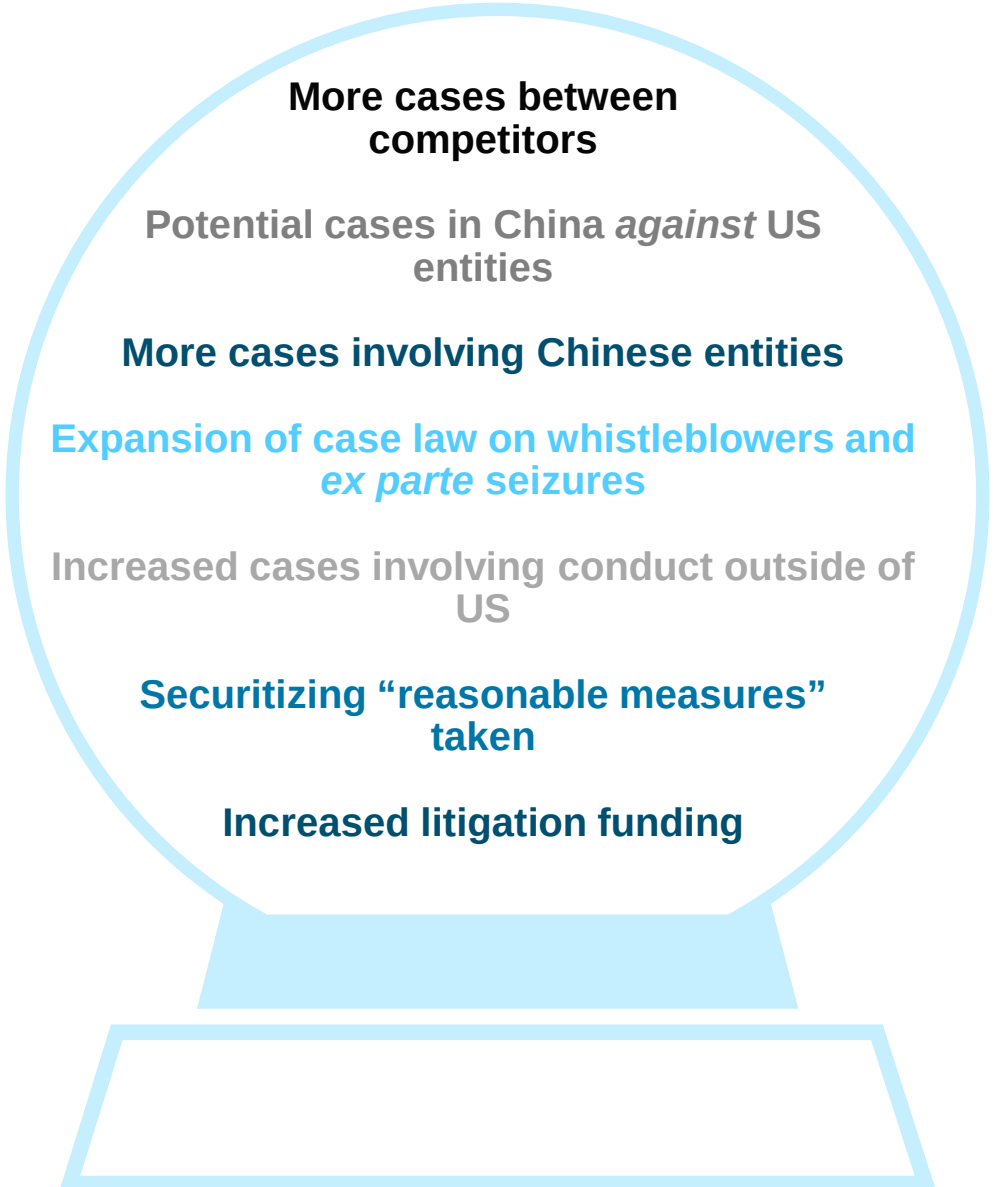
2. Utilize robust agreements and trainings clearly prohibiting use

3. Consider mechanisms to block/monitor uploads

PREDICTIONS

WINSTON & STRAWN LLP

What may the future hold?



WINSTON & STRAWN LLP

Questions?