KING & SPALDING

# Guarding Against and Responding to Trade Secret Theft:

## A Primer

**November 13, 2018**


**Michael Johnston**
King & Spalding

**John Horn**
King & Spalding

**Chris Burris**
King & Spalding

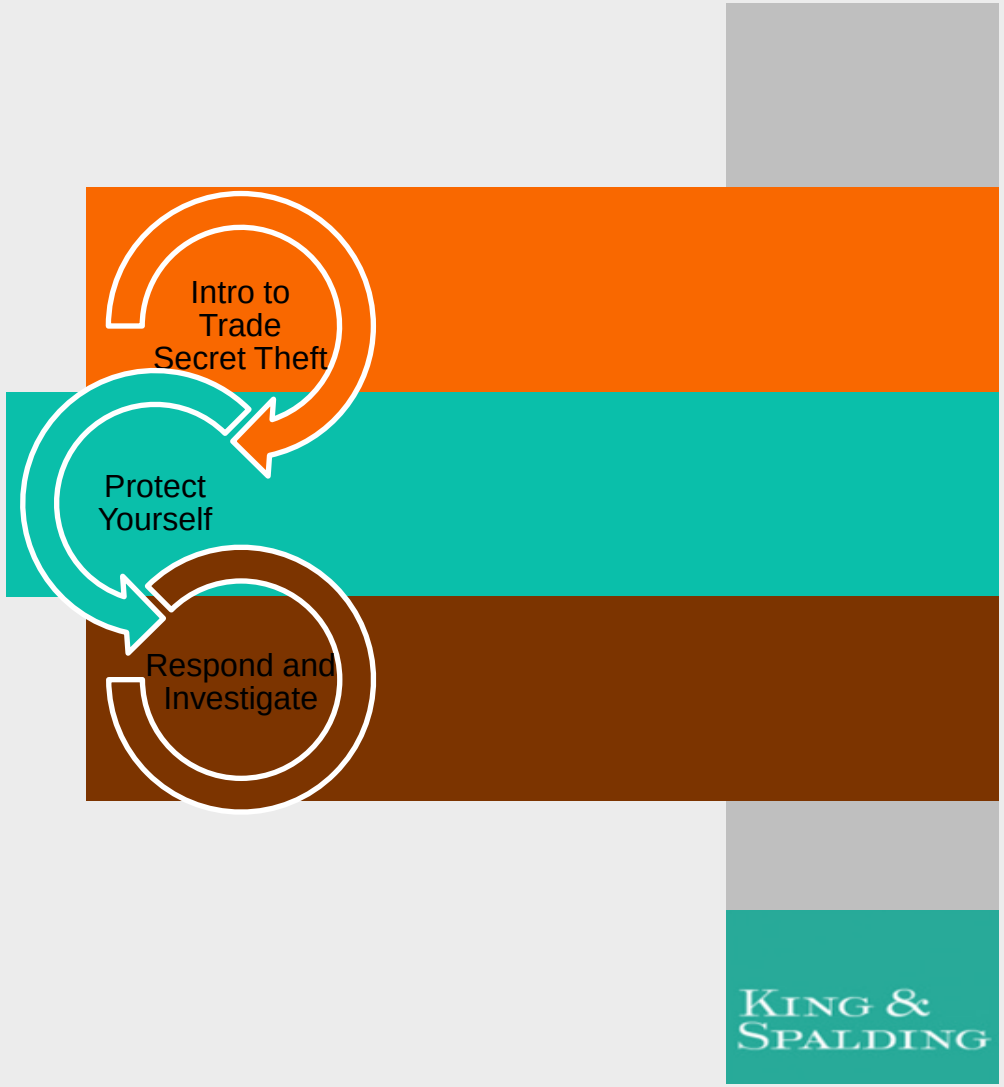

King & Spalding Pharmaceutical University

# Today's Roadmap

**What is trade secret theft – and what is the link to cybersecurity?**

**How can I protect myself and my company?**

**My trade secrets have been stolen – now what?**

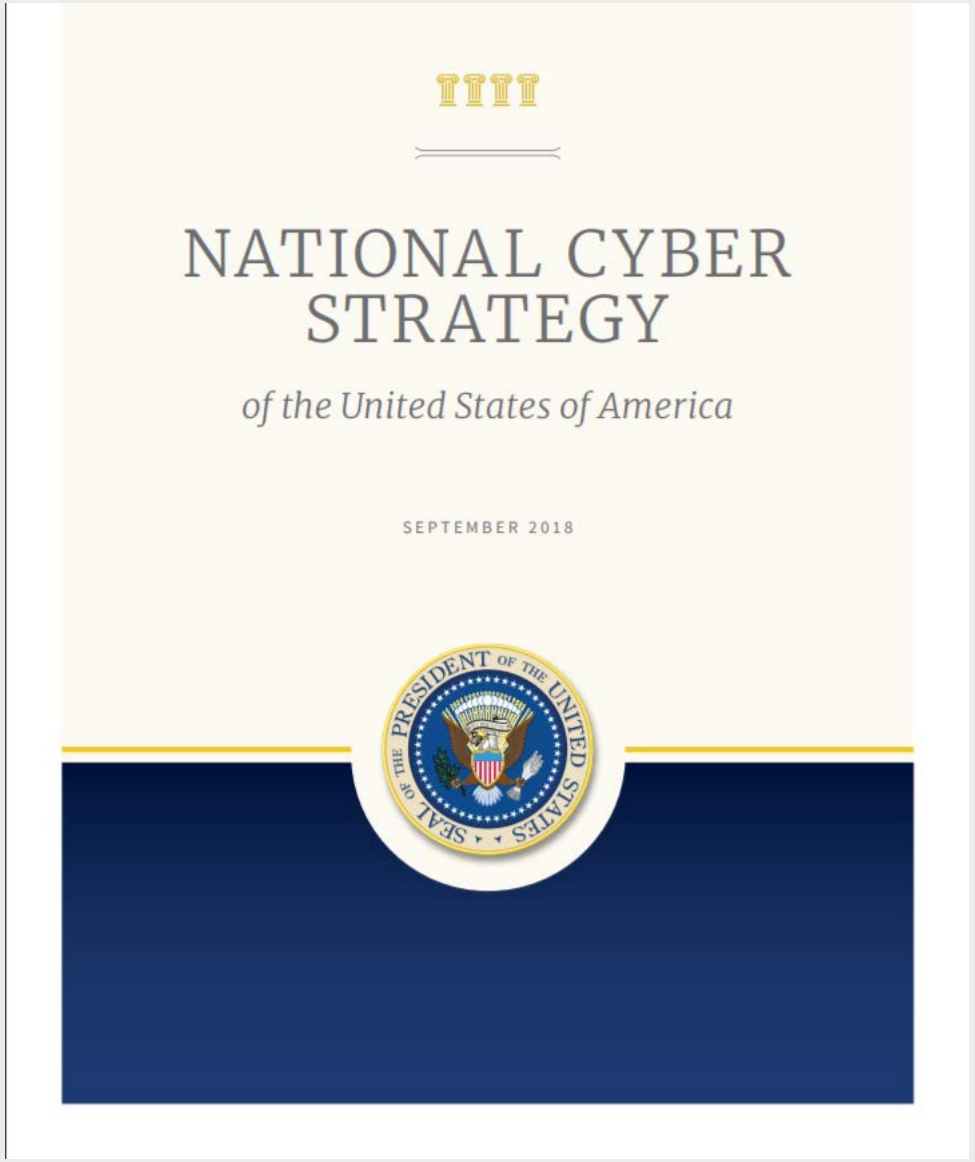


# Growing International Threats: Recent Examples


Intro to Trade Secret Theft

# 2018 National Cyber Strategy

- ✓ **Russia, China, Iran, and North Korea identified as the top 4 countries engaged in economic espionage, "often with a recklessness they would never consider in other domains."**
- ✓ **China alone identified as engaging "in cyber-enabled economic espionage and trillions of dollars of intellectual property theft."**



# Mechanics of the Threats

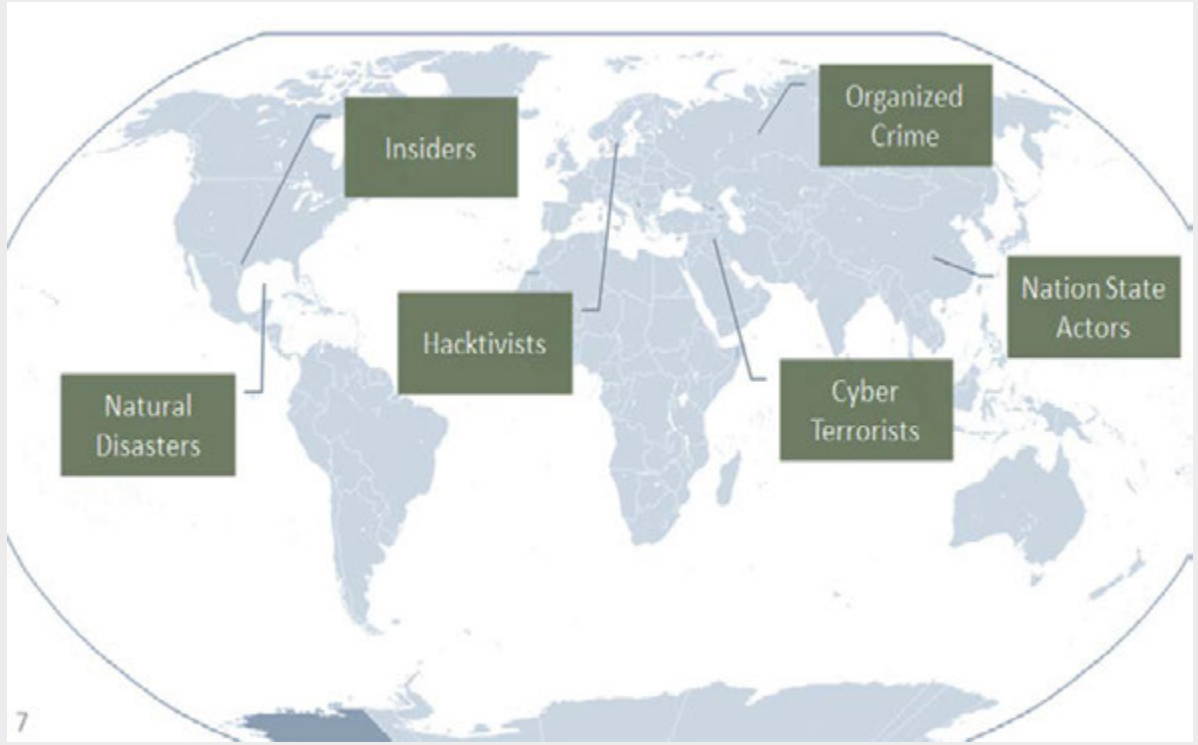
## Two main types of threats:

### 1. Outsider Threats

- Hacking
- Phishing
- Social Engineering

### 2. Insider Threats

- Nation-State Actor
- Disgruntled Employees



# Outsider Threats

## Cybersecurity

- Hacking
- Phishing
- Social Engineering Schemes

WANTED BY THE FBI

WANG DONG

**Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets**

**Aliases:** Jack Wang, "UglyGorilla"

**DETAILS**

On May 1, 2014, a grand jury in the Western District of Pennsylvania indicted five members of the People's Liberation Army (PLA) of the People's Republic of China (PRC) for 31 criminal counts, including: conspiring to commit computer fraud; accessing a computer without authorization for the purpose of commercial advantage and private financial gain; damaging computers through the transmission of code and commands; aggravated identity theft; economic espionage; and theft of trade secrets.

The subjects, including Wang Dong, were officers of the PRC's Third Department of the General Staff Department of the People's Liberation Army (3PLA), Second Bureau, Third Office, Military Unit Cover Designator (MUCD) 61398, at some point during the investigation. The activities executed by each of these individuals allegedly involved in the conspiracy varied according to his specialties. Each provided his individual expertise to an alleged conspiracy to penetrate the computer networks of six American companies while those companies were engaged in negotiations or joint ventures or were pursuing legal action with, or against, state-owned enterprises in China. They then used their illegal access to allegedly steal proprietary information including, for instance, e-mail exchanges among company employees and trade secrets related to technical specifications for nuclear plant designs. Wang controlled victim computers.

**If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.**

**Field Office:** Pittsburgh

Intro to Trade Secret Theft

KING & SPALDING

# Insider Threat Profiles and Motives

**Who is your insider threat?**

- Disgruntled Employees
- Disaffected Individuals

**Motivations**

- Disgruntlement
- Personal gain
- Ideology
- Competitive advantage or espionage

# Why Should Your Company Care?

1. **Increase in Cybersecurity Risks in General**

   The question is not if an organization will incur costs from cybersecurity breaches, but rather when and what magnitude.

2. **Increase in Monetary Costs of Trade Secret Theft**

   The harm to U.S. businesses from trade secret theft is hundreds of billions of dollars.

3. **Increase in Cyber Related Issues as the Direct/Indirect Causes of Trade Secret Thefts**

   Outside intrusions and insider thefts facilitated by breakdowns in internal controls.

# Legal Department's growing role…

**These issues fall within the core roles of in-house counsel**

- Align and prioritize cybersecurity and trade secret protection practices
- Coordinate the legal requirements for trade secret preservation with cyber security policies/controls.
- "Reasonable" protective measures are difficult to define and should be adopted in conjunction with legal guidance.
- Security measures must take into consideration privacy issues, employment law issues, etc.

**More regulators oversee data privacy and security and evaluate in legal terms**

# Trade Secrets

**Trade secrets may be the most vulnerable type of intellectual property.**

**Trade secrets derive value and retain legal protection only while they remain secret.**

**Data breach followed by public disclosure can undermine trade secret rights.**

# What Is a Trade Secret?

**Confidential information which provides an enterprise a competitive edge may be considered a trade secret. For example:**

- Sales methods
- Distribution methods
- Consumer profiles
- Advertising strategies
- Lists of suppliers and clients
- Manufacturing processes

# What Is a Trade Secret?

**The information must be secret (i.e., it is not generally known among, or readily accessible to, people that normally deal with the kind of information in question).**

**It must have commercial value because it is a secret.**

**It must have been subject to reasonable steps by the rightful holder of the information to keep it secret.**

# What Is a Trade Secret?

## State Level

Many states have adopted some version of the Uniform Trade Secrets Act (UTSA), or

Have a body of common law that provides protections to the trade secret owner.

## Federal Level

Passed Defend Trade Secrets Act in 2016, which provides additional avenue of protection for federal cause of action.

# Trade Secret Theft and the Pharmaceutical Industry

**Companies often rely on trade secrets to protect research and methodology that is not yet market-ready.**

**In such situations, companies need to be particularly sensitive to trade secret theft issues.**

**According to the Office of the National Counterintelligence Executive, clean energy technology and healthcare, pharmaceuticals, and related technologies are the top targets for foreign economic espionage of civilian technologies.**

**Pharmaceuticals are targeted primarily due to the massive R&D costs associated with new products and the growing need for medical care of aging populations in China, Russia, and elsewhere.**

# Protecting Against Trade Secret Theft

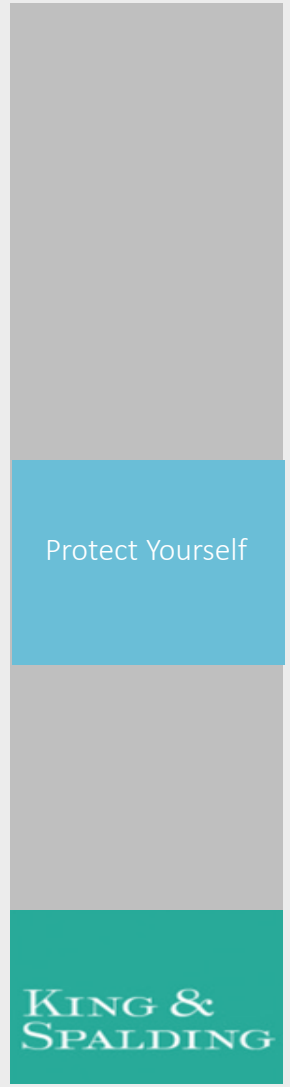
**The decision to preserve a trade secret should mandate escalated cybersecurity precautions.**

**Trade secrets should be segmented from the corporate network with restricted access.**

**Don’t only rely on NDAs (they do not help if signatories get hacked).**

**Collaborate internally to ensure level of protection is proportional to importance of trade secret.**

**Educate your employees.**



# Establish and Improve Your Cybersecurity Program

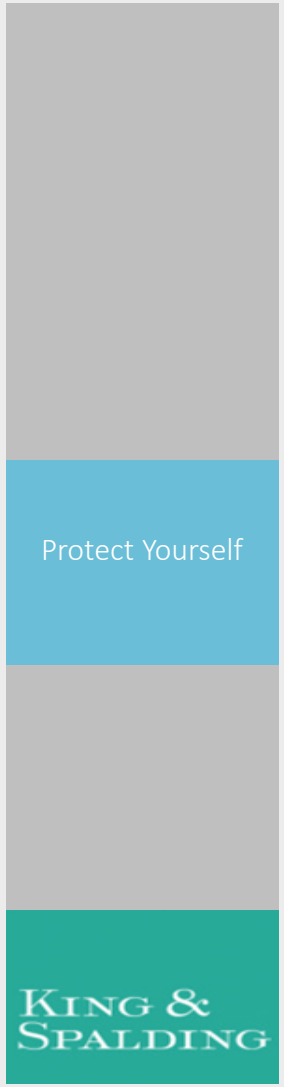
**The core components of a trade secret protection program mirror those denoted in NIST's Framework for Improving Critical Infrastructure Cybersecurity**


Protect Yourself

# Identify: What Assets Need Protection?

**It is important to identify trade secrets and then ensure that protections deemed reasonable by law are adopted to protect those secrets.**

**It is ill-advised to loosely view all corporate data as one big trade secret. Instead, particularly sensitive information such as source code or R&D work product should be stored in special repositories with heightened protections.**



# Identify, continued

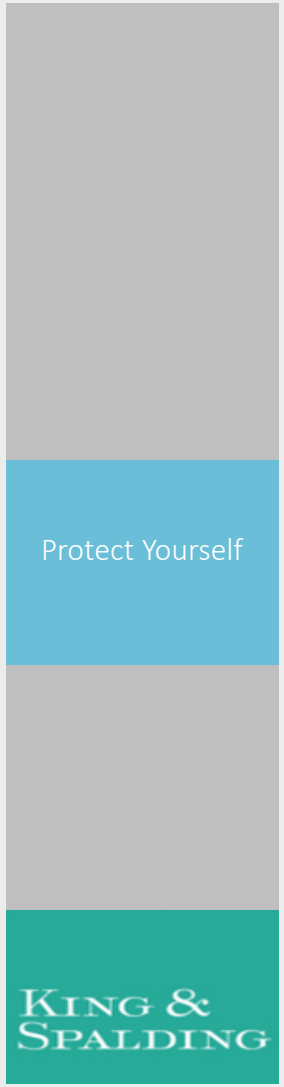
**Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.**

**Document, locate, label, and inventory the assets that need protection.**

**Determine where and how they are stored.**

**Determine who has access to them.**

**Continuously refresh this inventory to keep it up to date and complete.**

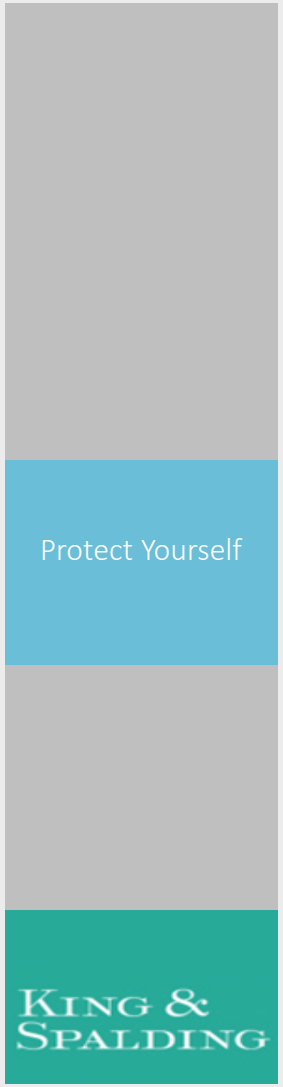


# Protect: Overview

**Develop and implement the appropriate safeguards.**

**Analyze existing protections such as security programs, procedures, and internal controls.**

**Assess vulnerabilities and strengthen your programs accordingly.**



# Protect: Overview, continued

**A good program will have technological, personnel, and physical security components. A solid program should:**

- Adopt employee policies that demonstrate the importance of cybersecurity and the trade secrets, and conduct trainings on the same
- Account for the relative value of the various trade secrets, and segregate and limit access to these categories
- Implement adequate password, firewall, encryption, and other technical defenses
- Adopt appropriate physical restrictions

# Protect: What Are Reasonable Efforts?

**The following security measures might be relevant to a determination of whether efforts taken were reasonable to maintain secrecy:**

- Restricted access
- Segregation from less sensitive data
- Electronic tagging of trade secret information
- Encryption especially with respect to mobile devices
- Complex password policy
- Electronic monitoring systems and data loss prevention
- Clear user policies
- Employee training

# Managing Insider Threat Risk: Where does your organization need to focus its resources?

| IDENTIFY | PROTECT | DETECT | RESPOND | RECOVER |
|---|---|---|---|---|
| | | | | |

- **Governance and C-Suite**
- **Policies, Procedures, and Internal Controls**
- **Tools and Technology/IT Security**
- **Threat Assessment, Analysis, Internal Security**
- **Training, Awareness, Communications**

Protect Yourself

KING & SPALDING

# Detect: What Techniques Can Identify Incidents?

**Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.**

**Recognize network anomalies in a timely manner.**

**Monitor information system and assets.**

**Maintain and test detection processes and procedures.**

**Many companies are turning to big data/Watson-type analytics to monitor employee activity on the network.**

# Role of Counsel

**It is important for counsel to work with IT, security, and the business groups who generate or control trade secrets to ensure that those secrets are identified and properly protected. Among other things, legal counsel should:**

- Identify critical assets requiring protection, such as business methods, sales strategies, and intellectual property;
- Collaborate on best practices to guard against physical and electronic theft;
- Draft employment agreements, company policies, and confidentiality and non-disclosure agreements for employees, customers, and third parties;
- Implement trade secret protection training programs for employees; and
- Coordinate trade secret protection plans and cybersecurity initiatives for compatibility and efficiency.

# Your Trade Secret Has Been Stolen: Now What?

**Trigger your incident response procedures.**

**Conduct a privileged investigation under the direction of counsel.**

- Consider engaging outside counsel.

**Consider legal obligations.**

- E.g., some public companies may have SEC disclosure requirements concerning the loss of intellectual property.

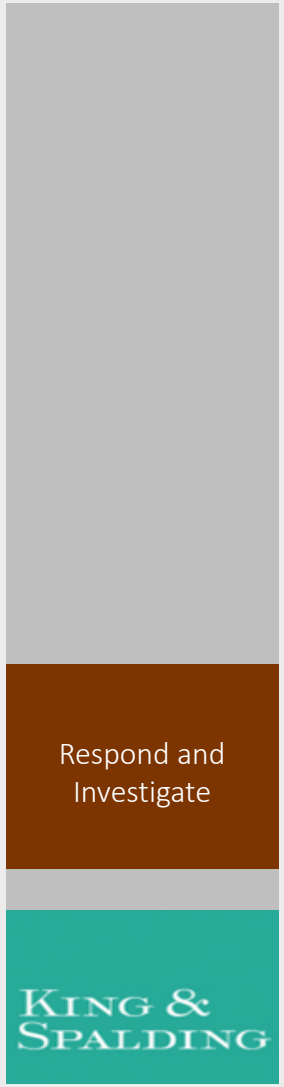
Respond and Investigate

KING & SPALDING

# Criminal Remedies

**There are pros and cons to going pursuing criminal remedies if your trade secrets have been stolen.**

| Pros | Cons |
| --- | --- |
| • The government has more resources<br>• Preservation of electronic records, warrants to get records, seizures of evidence<br>• If international, MLAT requests and extradition treaties | • You are turning the spotlight on yourself<br>• Privilege waiver issues<br>• Loss of control over the case and investigation<br>• Potential adverse publicity<br>• Reputational harm |



# Criminal Remedies

## CFAA Criminal Charges

It is a crime under the CFAA to access a computer without authorization or exceed authorized access and to thereby obtain information from a protected computer.

## Economic Espionage Act

Under the EEA, can bring charges for both:

- trade secret theft that would benefit any foreign government, instrumentality or agent, and
- misappropriation of trade secrets related to a product or service used or intended for use in interstate or foreign commerce.

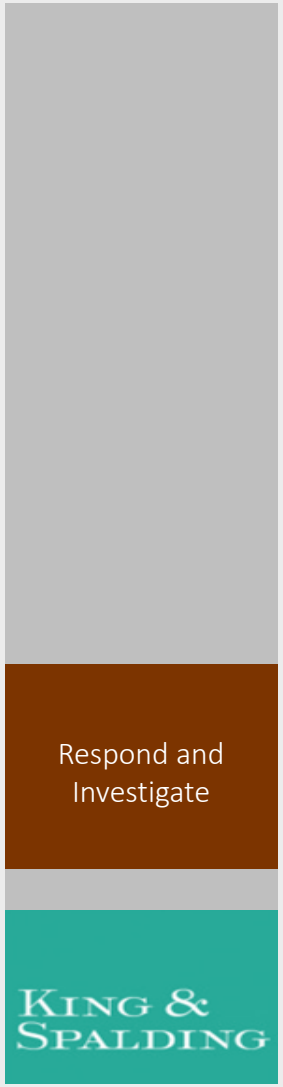
Respond and Investigate

KING & SPALDING

# Trade Secret Preservation

**If your trade secret is stolen, you want to preserve it as best as possible.**

- Seek injunctive relief through UTSA or DTSA (in conjunction with Federal Rule of Civil Procedure 65).
- Bring a Section 337 action in the International Trade Commission for an import ban against foreign goods incorporating misappropriated trade secrets.



# Civil Remedies

**Trade Secret Claim**

**Computer Fraud and Abuse Act**

**Violation of Non-Disclosure Agreement or Employee Contract**

**Violation of Fiduciary Duty**

**Tort: Conversion, trespass**

Respond and Investigate

KING & SPALDING

# Trade Secret Claim – UTSA

**The Uniform Law Commission's Uniform Trade Secrets Act is a model law which allows for an action for misappropriation by showing that the trade secret was:**

- acquired through improper means,
- disclosed or used by a party who knew it was acquired improperly,
- disclosed or used by a party who knew it was a trade secret and that it had been acquired by accident or mistake.

Respond and Investigate

KING & SPALDING

# Trade Secret Claim – State Law

**Most states have adopted some form of UTSA, although they vary.**

**Some states, like Florida, have enacted additional legislation providing a civil remedy to businesses who suffer a cyberattack.**

**The Defend Trade Secrets Act does not preempt state trade secret laws.**

Respond and Investigate

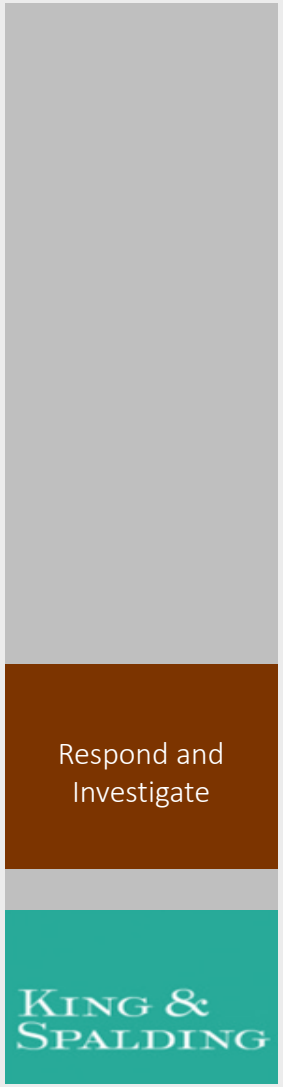
KING & SPALDING

# Trade Secret Claim – DTSA

**The Defend Trade Secrets Act is federal legislation based on UTSA. DTSA was signed into law on May 11, 2016.**

**DTSA creates a new, private federal civil action for "an owner of a trade secret that is misappropriated . . . if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce."**

**Injunctive relief may be permitted for the period of time it would have taken to independently develop the trade secret. Where injunctive relief would be inequitable, future use of the trade secret may be conditioned upon a reasonable royalty rate.**



# Computer Fraud and Abuse Act

**Under the CFAA, the owner of the trade secret may seek a civil remedy for obtaining information by intentionally accessing a computer without authorization or by exceeding authorized access.**

**There currently exists a circuit split in interpreting the CFAA's "exceeds authorization" provision to mean exceeding authorized access or merely authorized use.**

Respond and Investigate

KING & SPALDING

# Other Civil Claims

**If an employee stole the information, there could be a contract claim, a claim for violating an NDA (if one exists), or a violation of a fiduciary duty claim.**

- But, NDAs should not be viewed as complete protection because NDAs don't necessarily help if the third party is subject to a cyber-attack. Companies need to assess whether third parties have implemented security protections that measure up to internal requirements.

**Alternatively, a claim could be brought under tort law, such as for conversion or trespass.**

Respond and Investigate

KING & SPALDING

# Employee Agreements

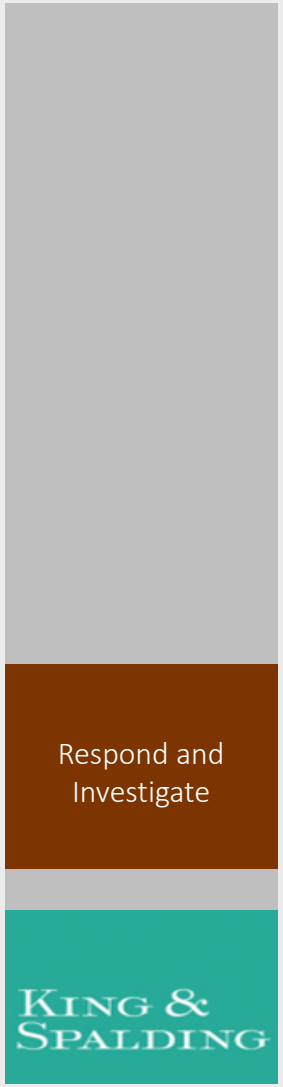
**Employee education is key.**

**Agreement better than policy.**

- Commitment
- Evidence

**Risks with agreements:**

- Too long: not followed
- Too specific
- Enforceability



# Employment Agreements, continued

**Detailed enough to educate, e.g.:**

> "Employer has developed commercially valuable technical and non-technical information."
>
> "The aforesaid information is vital to the success of the Employer's business."

**Provide examples, but not exhaustive list.**

**Administrative employees will have access.**

**Critical to show culture of organization.**

**Good forensic tools for monitoring/identification.**

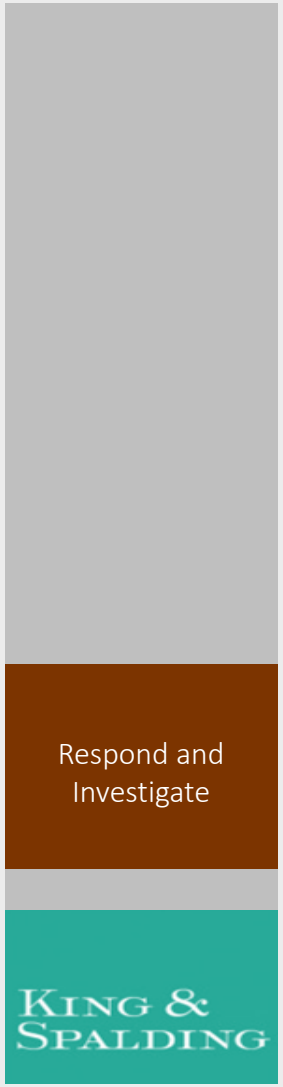
# Education, Training, & Exit Interviews

**Education & Training for new and current employees:**

- Orientation
- Informal Reminders
- Formal follow-up
- Mandatory and documented attendance to trainings

**Exit Interviews:**

- Gathering information
- Policy reminder
- Return of materials
- Reaffirm written commitment
  - Avoid inconsistent application

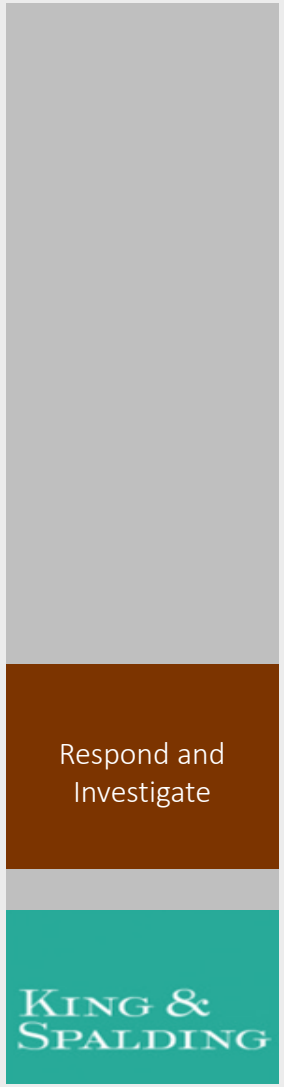


# Policies

**Policies** reinforce agreements, serve as an opportunity for education, and need to match operations and business realities.

**Distribution of Policy:** Require Proof of receipt and acknowledgement. Keep records.

**Update Policies** to reflect changes in confidential information. Keep in mind new storage methods and improvements to protective measures.



KING & SPALDING

# Guarding Against and Responding to Trade Secret Theft

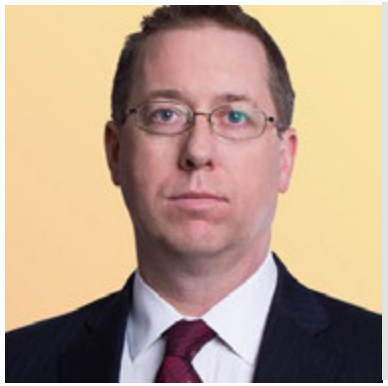
## Questions?

**Michael Johnston**

mjohnston@kslaw.com
(404) 572-3581

**John Horn**

jhorn@kslaw.com
(404) 572-2816



**Chris Burris**

cburris@kslaw.com
(404) 572-4708

**November 13, 2018**

King & Spalding Pharmaceutical University