Seyfarth

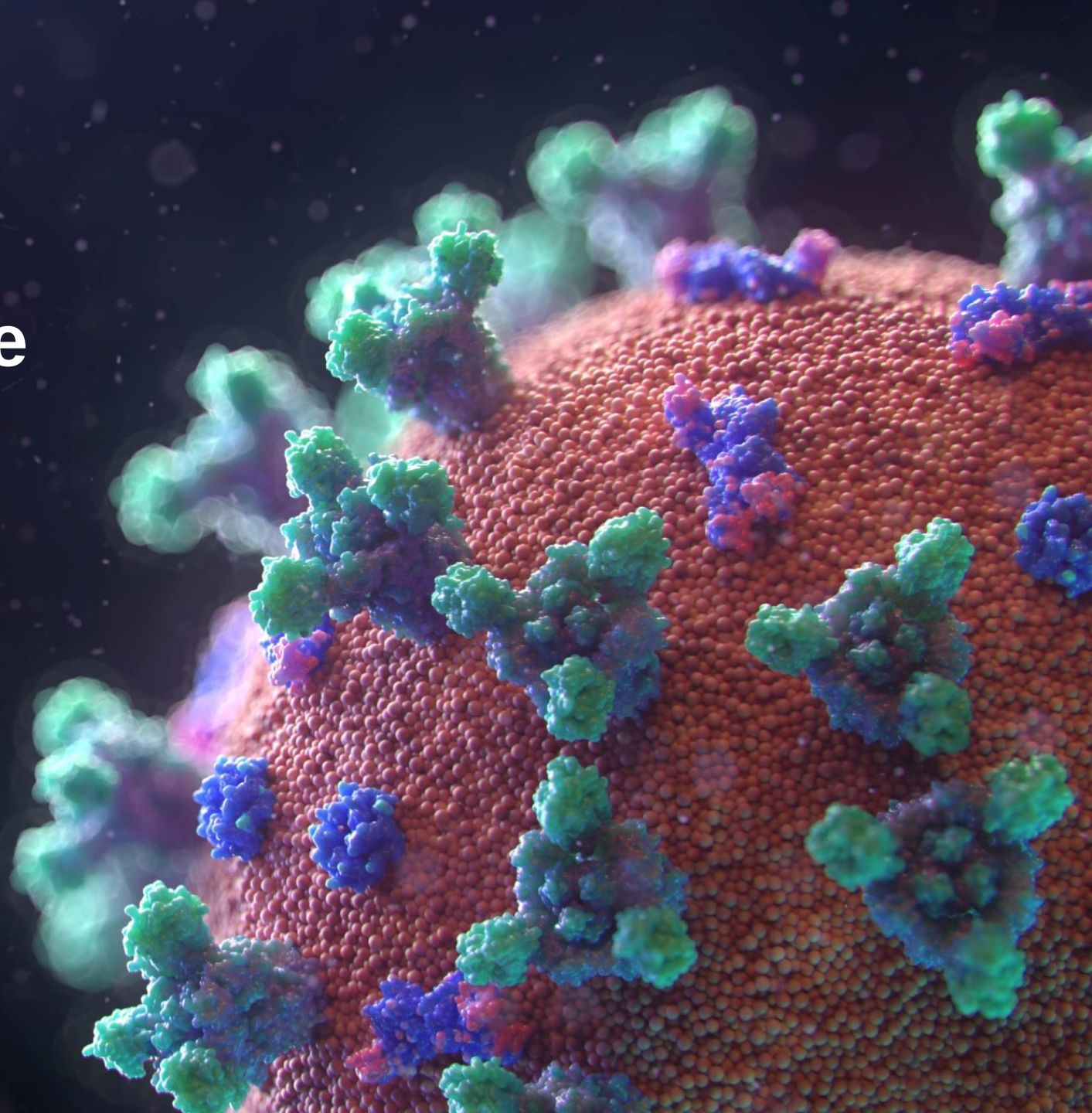
# Coronavirus & Remote Work Force: Best Practices for Protecting Trade Secrets and Intellectual Capital

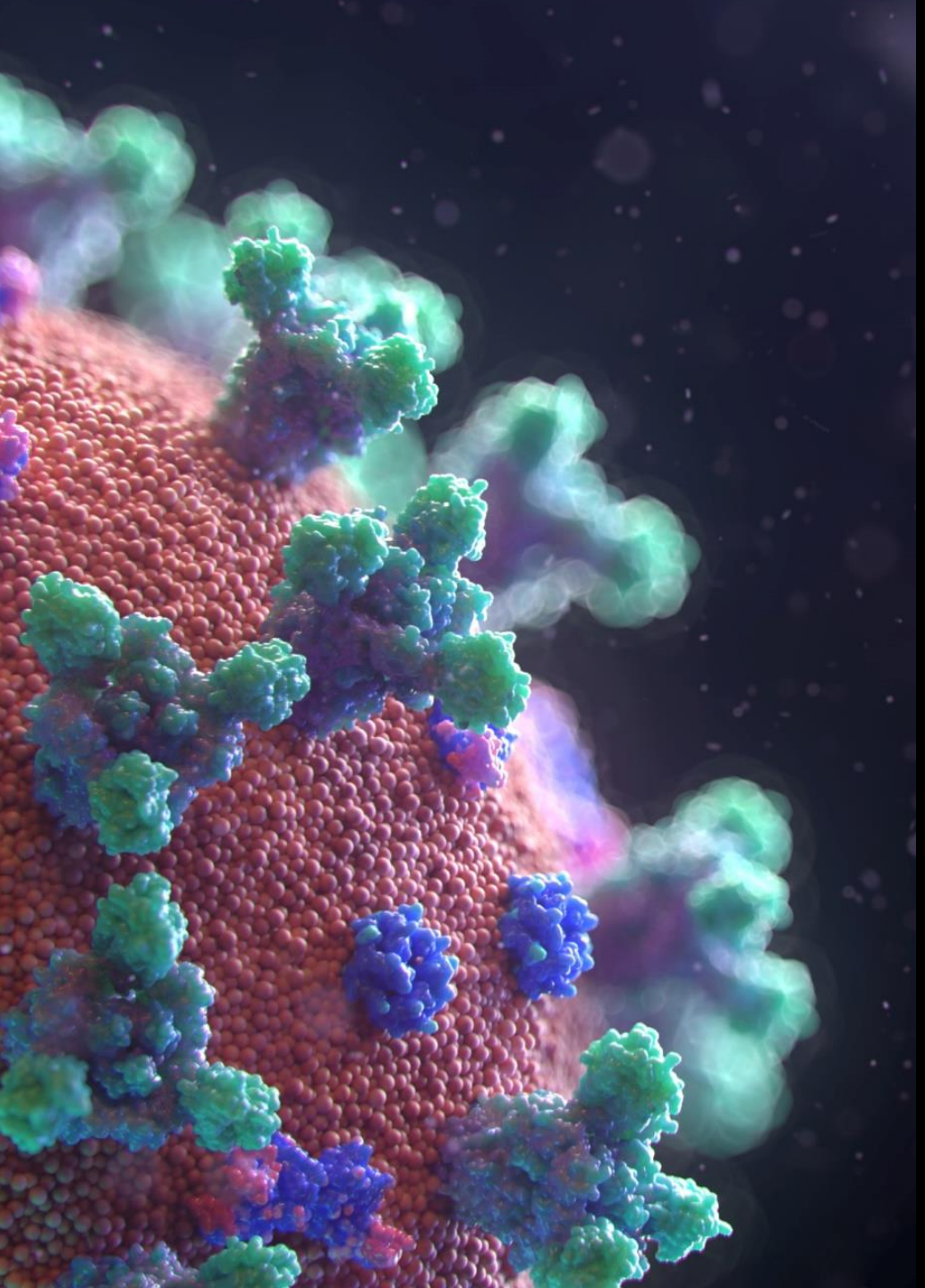
Michael Wexler
Jesse Coleman
Justin Beyer

March 27, 2020

**Seyfarth Shaw LLP**







**Visit our COVID-19 Resource Center to sign up for daily updates:**

www.seyfarth.com/covid19

Seyfarth

# Legal Disclaimer

This presentation has been prepared by Seyfarth Shaw LLP for informational purposes only. The material discussed during this webinar should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The content is intended for general information purposes only, and you are urged to consult a lawyer concerning your own situation and any specific legal questions you may have.

**Seyfarth Shaw LLP**

# Objectives

01 What Are The Unique Challenges of Coronavirus?

02 What Needs Protection?

03 Why Does This Matter?

04 What Do You Have In Place ?

05 What Should You Be Doing Now?

# Speakers

**MICHAEL WEXLER**
Litigation Partner
CHICAGO

**JESSE COLEMAN**
Litigation Partner
HOUSTON

**JUSTIN BEYER**
Litigation Partner
CHICAGO

**MICHAEL WEXLER**
Litigation Partner
CHICAGO

- Michael is Chair of the Trade Secrets, Non-Compete and Computer Fraud Practice Group, a former prosecutor, experienced trial attorney, counselor and litigated some of the most high profile trade secret and non-compete matters in the country. He can be reached at (312) 460-5559, mwexler@seyfarth.com.

- He litigates injunctions, TRO's and jury trials throughout the United States in numerous substantive areas including technology, healthcare, finance, pharma, medical devices, cloud computing, defense, criminal and more. Michael also drafts and counsels clients regarding agreements, policies, executive compensation, equity awards, hiring, separation and acquisitions.

**JESSE COLEMAN**
**Litigation Partner**
**HOUSTON**

- Jesse is Co-Chair of the Healthcare Practice Group and a Partner in the Trade Secrets, Non-Compete and Computer Fraud Practice Group. He is based in Houston, Texas and is an experienced trial attorney and counselor. Jesse can be reached at (713) 238-1805, jmcoleman@seyfarth.com.

- He advises health care clients and businesses in all sectors of the world economy on trade secret and restrictive covenant matters. He litigates injunctions and tries cases throughout the country in state and federal court.

**JUSTIN BEYER**
**Litigation Partner**
**CHICAGO**

- Justin is a trial attorney and counselor in the Trade Secrets, Non-Compete and Computer Fraud Practice Group as well as the General Commercial litigation group. He can be reached at (312) 460-5957, jbeyer@seyfarth.com.

- He litigates injunctions and trials in numerous jurisdictions and industries throughout the United States including the substantive areas such as finance, medical devices, cloud computing. Justin also drafts and counsels clients regarding agreements, policies and hiring related issues.

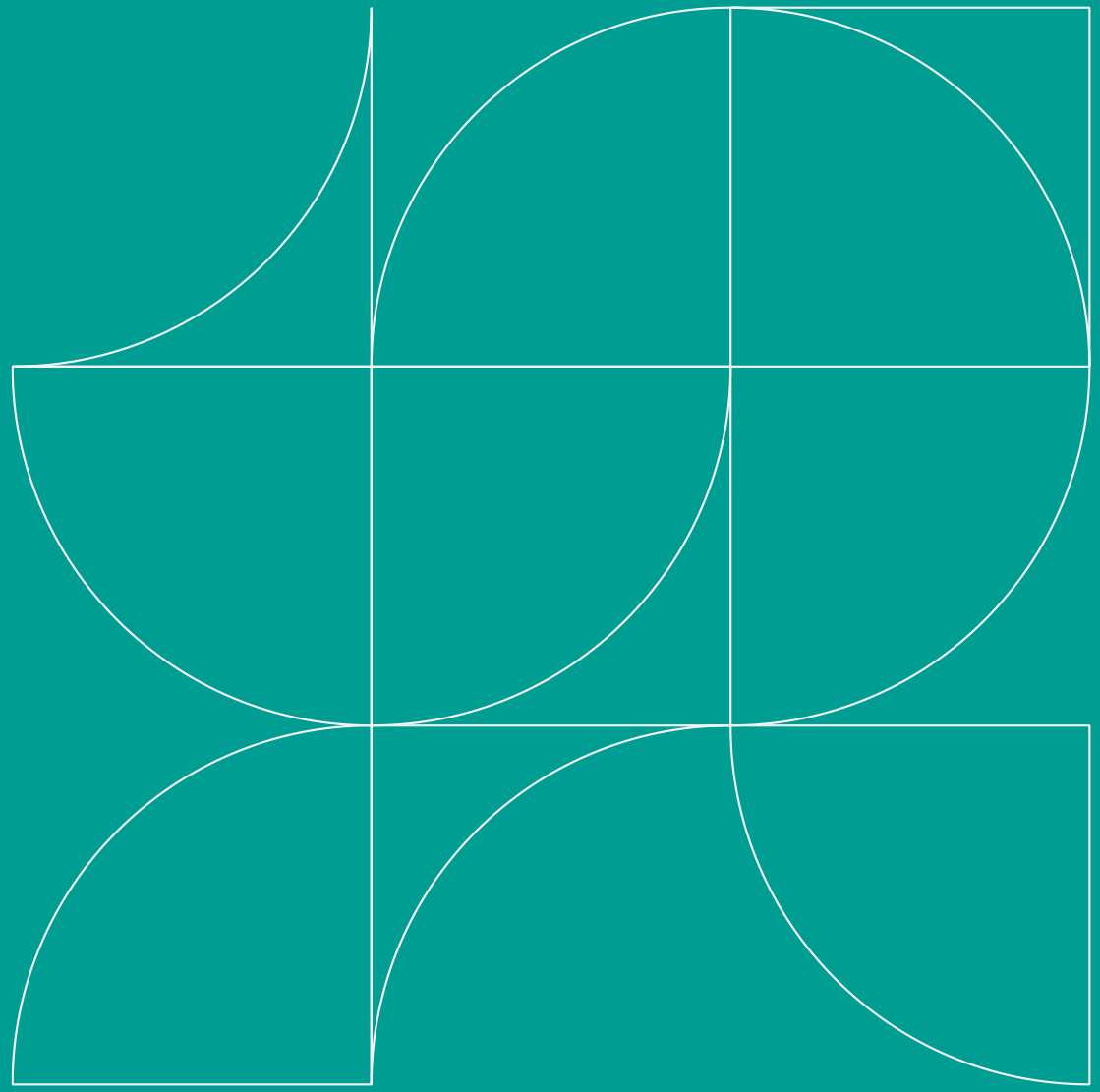
# **Coronavirus:**
Unique Challenges & A Remote Work Force

## *A Trade Secret…*

… is one of the most elusive and difficult concepts in the law to define.

*Learning Curve Toys Inc. v. PlayWood Toys, Inc.,* 2003 U.S App. LEXIS 16847 (Aug. 18, 2003)

# What Are The Unique Challenges Of Coronavirus?



# UTSA
## Definition of "Trade Secret"


## A "Trade Secret" is:

information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and,

(ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."

# The Defend Trade Secrets Act of 2016

## Definition of Trade Secret

**"Trade secret"** includes all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—

a) the owner thereof has taken **reasonable measures** to keep such information secret; and

b) the information derives **independent economic value**, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic

# What is a Trade Secret?

- Trade secrets = information
- Generally **not known** to others
- Economically valuable (actual or potential)
- **Reasonable efforts** to maintain secrecy

# Trade Secrets Must Be Kept Secret!

- Public disclosure of a trade secret destroys the information's status as a trade secret. *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1002 (1984)

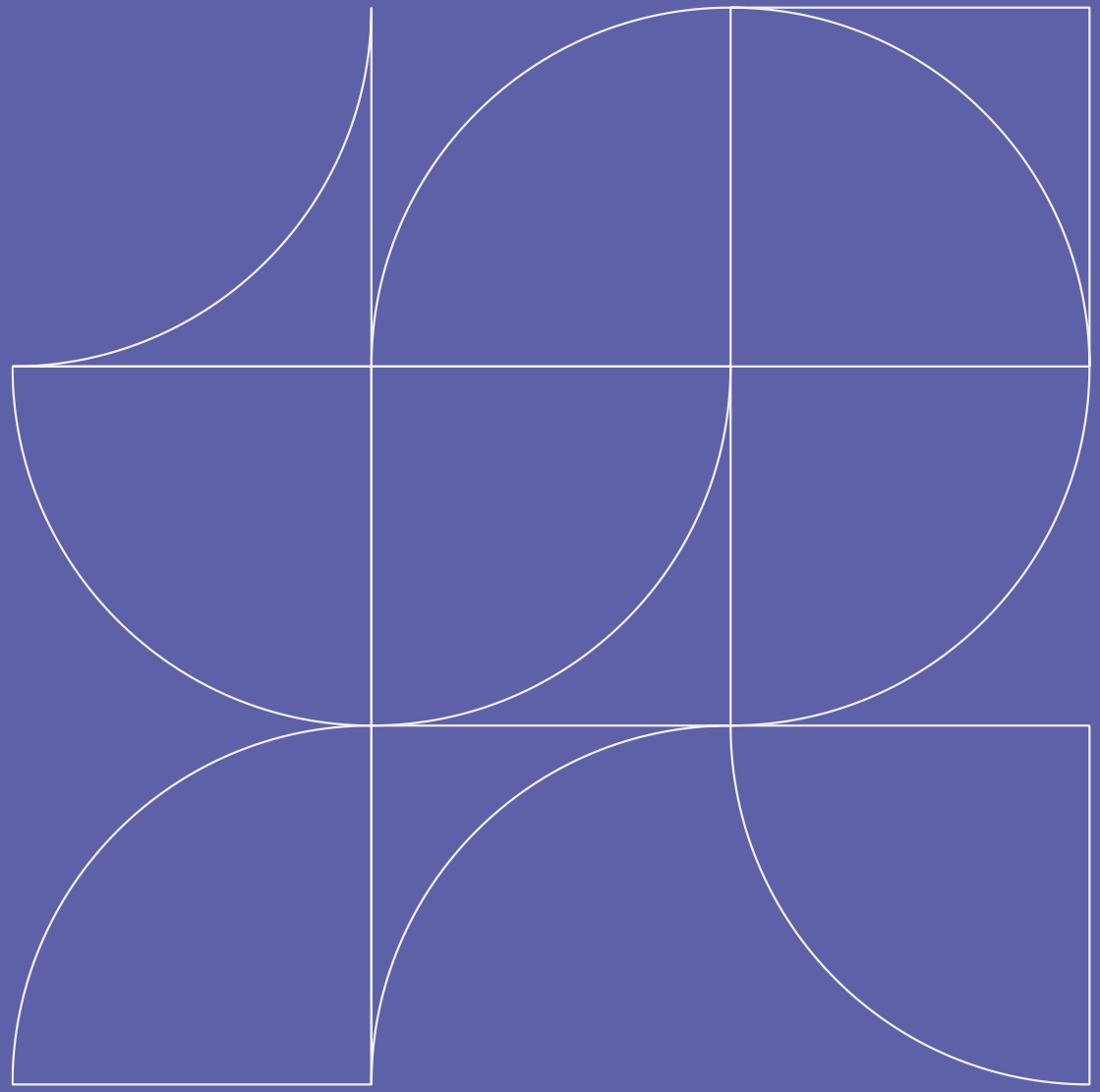
- "It is axiomatic that without secrecy, no trade secret can exist." *BDT Products, Inc. v. Lexmark, International, Inc.*, 274 F. Supp. 2d 880, 891 (E.D. Ky. 2003)

- Between 2009 and 2018, 15% of trade secret cases were dismissed because the plaintiff did not take reasonable measures to protect its trade secrets. And Defendants were successful in 54% of the cases that went to verdict between 2016 and 2018

# What Level of Security is Required?

- Absolute secrecy and heroic measures are not required – only measures that are "***reasonable under the circumstances***."
- Prevention protocols are key.
- However, if a trade secret is leaked and the company does not try to fix the leak and minimize damage, its value to the company may be severely compromised and lost forever.
- Courts will carefully scrutinize whether the company took appropriate steps to safeguard security.

# What Needs Protection?



# Identifying Trade Secrets

**Factors That Help Determine Whether Information is a Trade Secret:**

- Extent known outside the company
- Extent known by employees and others inside company
- Measures taken by company to protect secrecy
- Value of trade secret to company and competitors
- Time, effort, and money expended in development
- Ease with which it can be properly acquired or duplicated by others (reverse engineering/independent derivation)

# Examples of Information that May Be Trade Secrets

- **Internal Customer Lists**
  - High-trading or high-net-worth clients and their order histories;
  - Institutional fund clients, pension fund clients, and their portfolio allocations;
  - Angel / venture capital investors and their propensities;
- **Internal Modeling Documents**
  - Cash-flow forecast models;
  - Options / futures pricing models;
  - Underwriting models;
  - Analytics compilations and modeling;
- **Internal Opportunities and Trends**
  - SWOT analyses;
  - Future private-equity targets;
  - Emerging markets.

# Examples of Trade Secrets

- Product Formulas
- Manufacturing Processes
- Marketing Strategies
- Business Plans
- Sensitive Financial Information
- Pricing/Cost Information
- Unique Software & Source Code
- Knowledge About Customers (e.g., requirements, preferences, order history, purchasing trends)
- Negative Research Results
- Know How

What is the **economic impact of trade secret theft** to U.S. companies?

Estimates of trade secret theft range from:

# *1 - 3%*

of the Gross Domestic Product of the United States and other advanced industrial economies*

**CREATe and PwC: "Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential threats (2014)*

# External Threats

to Corporate Confidential Information

**Cyber threats can threaten the trade secret eligibility for company information:**

– "Once a trade secret is posted on the Internet, it is effectively part of the public domain, impossible to retrieve. . . . [T]he party who merely down loads Internet information cannot be liable for misappropriation because there is no misconduct involved in interacting with the Internet." *Religious Tech. Ctr. v. Lerma* (E.D. Va. 1995).

– Potential Shift in Law – What used to constitute "reasonable measures" to maintain secrecy may no longer be reasonable as cyber threats become more universal and apparent.

# **Typical Measures** to Protect Trade Secrecy Should Include:

- **Agreements with Employees**
  - Offer letters
  - NDAs, Return of Materials, Post-Employment Restrictive Covenants
- **Employee Policies and Handbooks – Written and Available**
  - Confidentiality, Privacy, BYOD
  - Include certifications of receipt/review
- **Confidentiality Agreements with Third Parties**
  - Clients, vendors, contractors, suppliers, JV partners
  - Due diligence parties – targets, acquirers, underwriters
- **Secure network and facility**
  - Password protection of hardware and software
  - Need-to-know distribution of materials
  - “Lock and Key”
  - Monitoring tools (real time and after-the-fact)

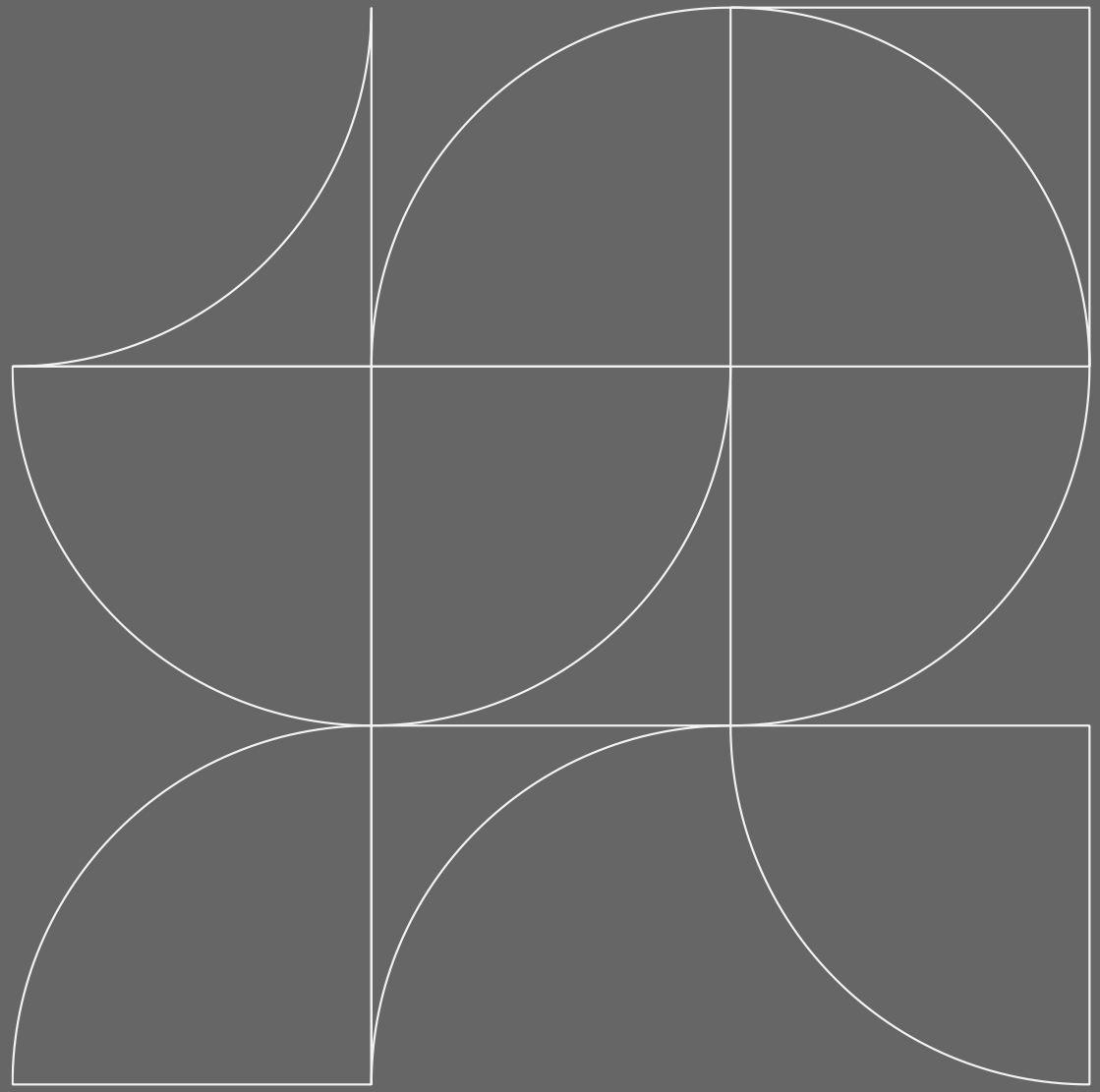
# Protection = Reasonable Efforts to Maintain Secrecy

**Take actual efforts to maintain secrecy, including:**

- Confidentiality agreements = leading indicator
- Information security
  - Password protection
  - Email and electronic data policies (beware of BYOD)
  - Confidentiality reminders on screens and documents

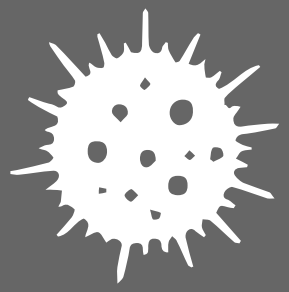
- Limit access—need to know/tiered access
- Must take action against breaches (does not always require filing suit)
- Regular training on policies (consider trackable e-modules)
- Onboarding, exit interviews, and related documentation (audit this)
- Limit information made available to vendors and subcontractors and have appropriate contracts with vendors

# Why Does This Matter?



# **Coronavirus:** Displacing Safe Work Environments

# Coronavirus



## LATEST UPDATES

As of 7:30 a.m. Central Today

- Number of cases – 549,604 cases
- Number of deaths – 24,863 deaths
- Number of recoveries – 127,531
- US has surpassed China as the country with the greatest number of cases

# Efforts to Keep the Disease from Spreading

- A ***third*** of the global population is on coronavirus lockdown
- 46 states have issues stay-at-home orders or placed limits on gatherings
- HHS/CDC recommend staying at home, engage in “social distancing”
- Major information companies (Amazon, Twitter, Facebook, Google, Microsoft) have instructed non-essential people to work from home

# HIPAA

Effective March 15, 2020 and throughout the duration of coronavirus pandemic, HHS has waived penalties against covered hospitals that fail to comply with the following provisions of the HIPAA Privacy Rule:

- the requirements to obtain a patient's agreement to speak with family members or friends involved in the patient's care;
- the requirement to honor a request to opt out of the facility directory;
- the requirement to distribute a notice of privacy practices;
- the patient's right to request privacy restrictions; and
- the patient's right to request confidential communications.

"This week, it's going to get bad. ... We really, really need everyone to stay at home."

U.S. Surgeon General Jerome Adams

**“We can’t close. It will kill us.”**

Executive of large company

# **Heightened risks**

to trade secrets misappropriation or loss as a result of COVID-19

- Remote working environments increase the use of:
  - unsecure personal and public wi-fi networks
  - unsecure personal devices
  - unsecure personal email accounts to transfer corporate data
  - syncing with unsecure personal cloud storage accounts
  - unsecure printed materials
  - unencrypted portable electronic storage devices
  - unsecure connections to employers systems (remove desktop software)
  - unsecure conference call lines
- Increased visibility in public locations of confidential information
- Increase phishing schemes and other fraud

Companies Must Make Sure that They Are

# Keeping Trade Secrets a Secret

Public disclosure of a trade secret destroys the information's status as a trade secret. *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1002 (1984)

"It is axiomatic that without secrecy, no trade secret can exist." *BDT Products, Inc. v. Lexmark, International, Inc.,* 274 F. Supp. 2d 880, 891 (E.D. Ky. 2003)

# Reasonable Efforts to Protect Trade Secrets

- Is access to the information restricted to only those employees who need access to it?
  - Tiered access
  - Appropriate contracts with vendors
- Do the employees who have access to the information sign confidentiality agreements *before* having access to those materials?
- Is the material marked "confidential"?
- Is it something that employees openly discuss around third parties?
- Is there a written company policy?
- Are company documents accessible remotely? If so, are home computers safeguarded?
- Training
- Actions taken against breachers

**Best Practices:**
Protecting Your Information **(ACE)**

*Consistency is Key*

**A**udit

**C**reate A Culture Of Confidentiality

**E**nforce


# Create a Culture of **Confidentiality**

- Ensure employees understand what the company considers confidential, and why it is important to maintain confidentiality
  - Tie it in with client service
  - And make sure to get it back
- Treat others how you would like to be treated!
- Provide training modules with examples of “dos” and “don’ts”
  - Identify industry standards
- Mark things confidential/proprietary
- Make security protocols easy to understand, familiar, and uniform

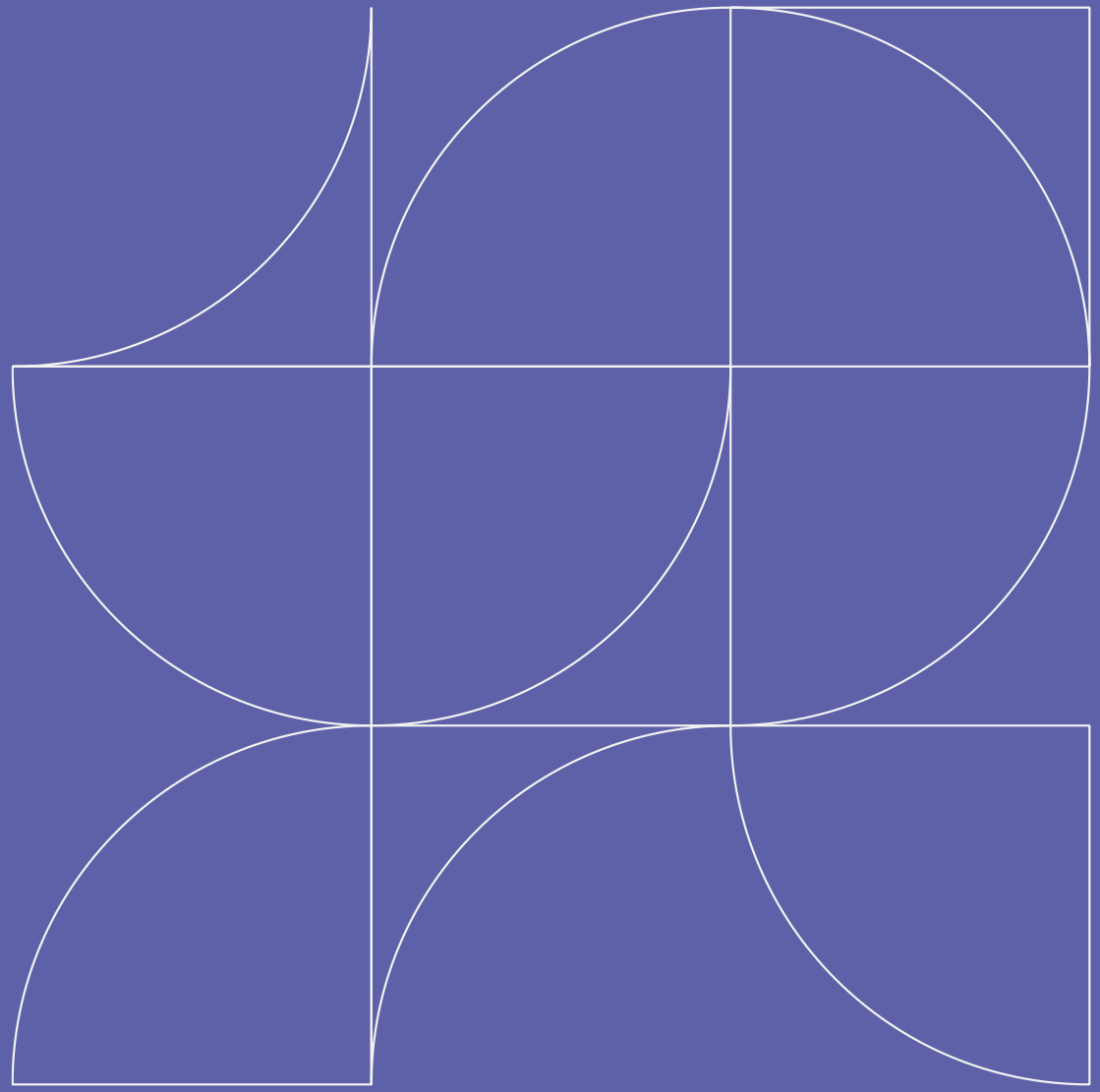
# COVID-19 Measures

- Global pandemic and immediate work-from-home orders stressing infrastructures

- Requiring businesses to nimble in their responses
  - How are you addressing teleconferencing
  - How are you addressing communicating out of office/off network
  - What policies do you have in place for working on non-company devices
  - Are you addressing employees utilizing unsecure networks or less secure ones
  - Are you stressing best practices for use/dissemination of confidential information?

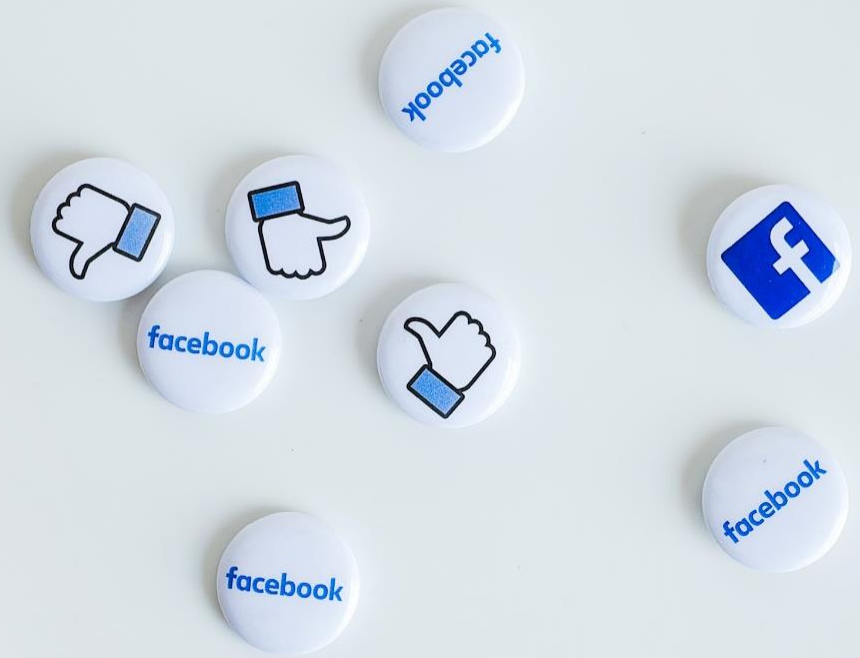
- **Must continue to protect trade secrets**

# What Do You Have in Place?



# Employee Agreements

- Confidentiality Agreements
- Return of Materials Agreements
- Invention Assignment Agreements
- Restrictive Covenants Agreements
  - Non-compete
  - Forfeiture for competition
  - Customer non-solicit
  - Employee non-solicit
  - No-hire
  - Non-disclosure

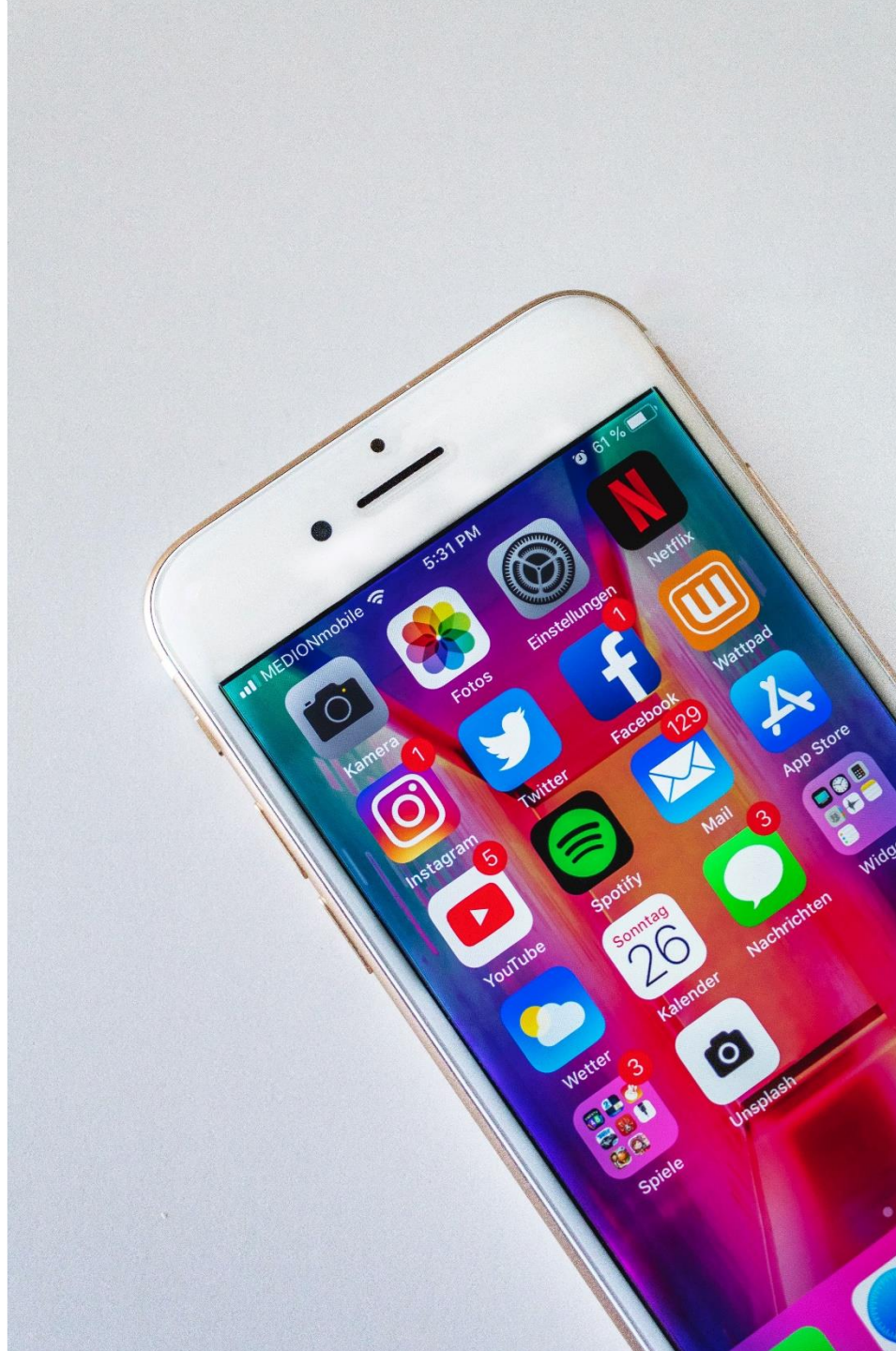



# Social Media Policies

- Do you have a social media policy that covers confidential information?
- Reasonable policies commensurate with threats
  - Ensure that policy is not overbroad
    - E.g., National Labor Relations Act §7 protects employee rights to engage in concerted activities
- Provide specific definition of confidential information and provide examples
  - Ensure that the policy is well-communicated and explained to employees
  - Have separate ownership of company social media account agreements

# BYOD Policies

- Do you already have a BYOD policy?
- Different policies for different levels of employees?
- If you have a BYOD policy:
  - ✓ Specify which devices are permitted
  - ✓ Provide clear restrictions regarding use/transfer of company data
  - ✓ Explain when company gets access to device and data
  - ✓ Incorporate into exit interview process
  - ✓ Explain investigation, incident remote wiping procedures
- Does this need to be revamped/modified for current situation?



# Employee Handbook

- Do you have one?
- How does it align with mass work-from-home needs?
- Does it need to be revamped?
- Do certain provisions need to be relaxed?
- Can certain provisions be highlighted to address employees unfamiliar with robust confidentiality protections?

# Information Security Policy

- Do you have one?
- What information in this policy must be communicated to employees?
  - What steps have you taken to communicate policy?
  - Explain policy?
  - Ensure understanding by employees?
- Is there any provision inconsistent with new reality?
  - If so, has company decided how it should be relaxed/reconciled?

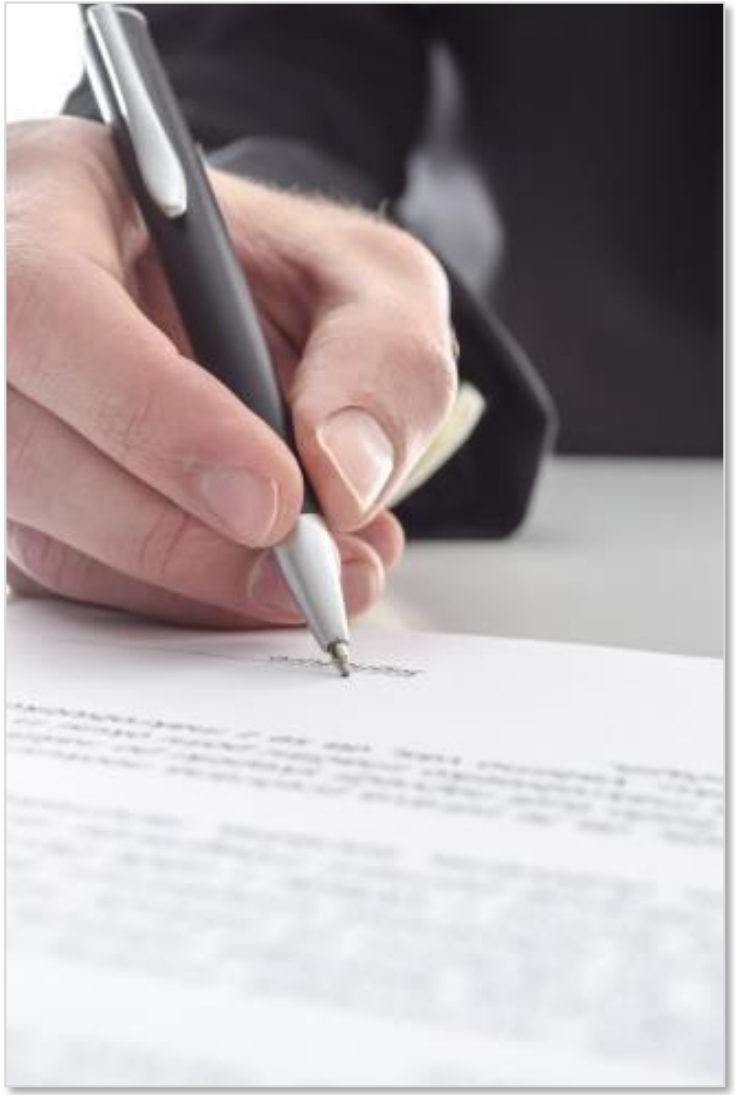
# What To Do If With/Without These Policies

- Remind employees of these policies
  - Company wide distribution *in writing*
- Use Time to Remind Employees of Obligations
  - Hold a teleconference to address obligations (what is confidential, how to protect)
- Even if you lack policies, be proactive
- Communicate expectations about
  - device usage and best practices
  - where they hold video conference calls
  - best off-site work practices
  - how to protect information
- Formalize new policy and roll-out
- Send emails outlining company best practices (if no formal policy exists)
- **Don't let work-from-home environment erode/eliminate confidentiality efforts**

# On-Boarding Procedures

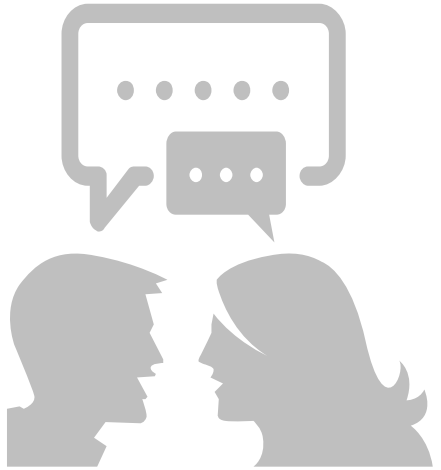
## What agreements should be in place for particular employees?

- Non-disclosure and trade secret protection covenants?
- Non-compete covenants?
- Invention assignment agreements?
- Acknowledgement that employee will not use prior employers' trade secrets and confidential/proprietary information and has returned all company property?
- Computer use and access agreements?
- Social media ownership and policies?



# Exit Interviews & Processes

- Must adapt due to inability for in-person exit interview
- Prepare for the interview, identify the trade secret and confidential information the employee accessed/used, consider having in-house counsel or HR and employee's manager present as appropriate
- Question the departing employee in detail
  - Ask employee why s/he is leaving
  - Ask employee what new position will be
- Check employee's computer activities and work activities in advance of the meeting
- Ensure that all company property, hardware, and devices have been returned, including email and cloud data, and social media accounts; consider using an inventory list
- Offer to have materials picked up from house, if necessary



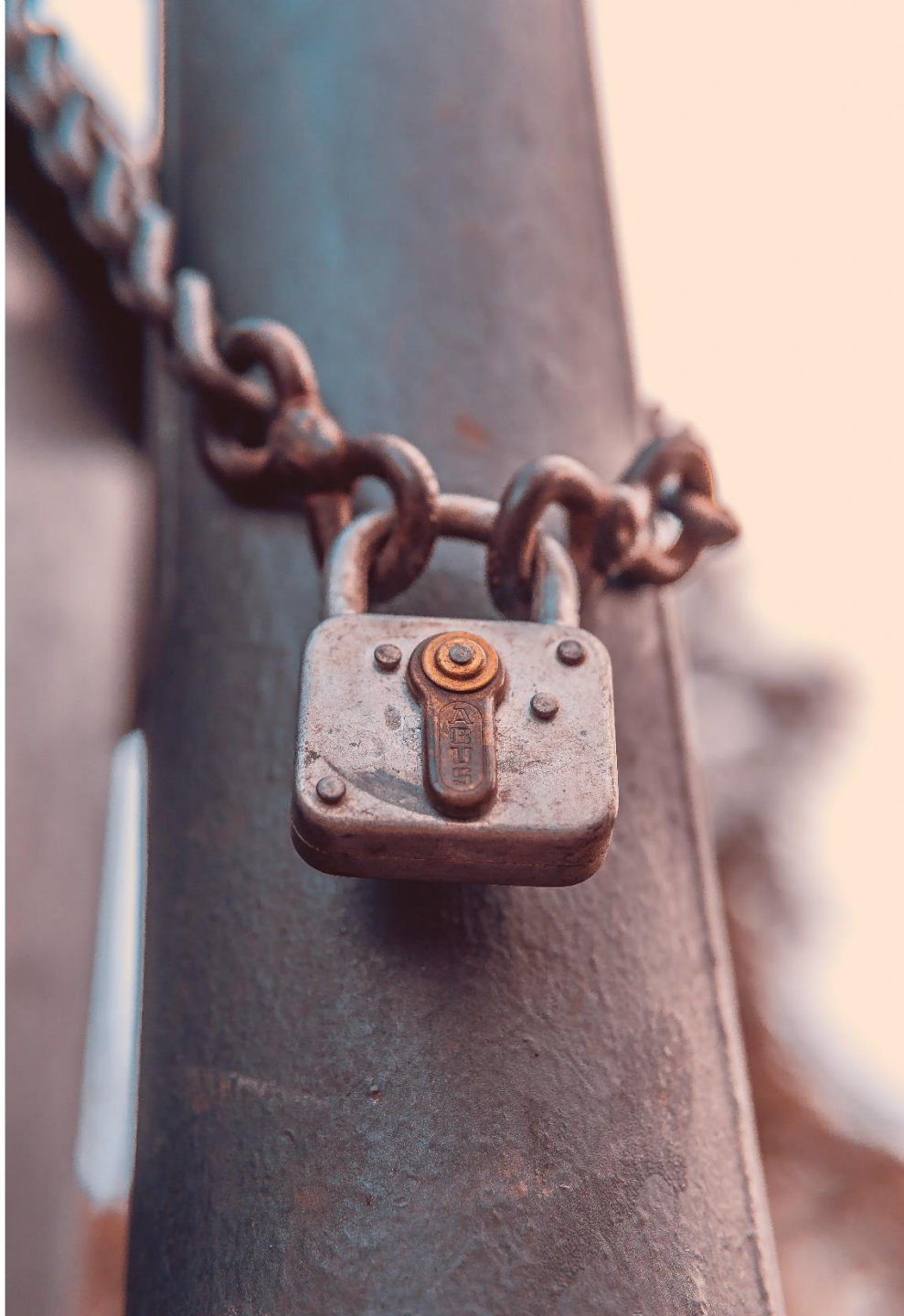
# Exit Interviews & Processes

- Ensure that arrangements are made to have all company data removed from any personal devices
- Disable access to company computer networks
- Make sure you obtain user names and passwords for all company social media accounts
- Inform the employee of continuing obligations under agreements with the company
- Consider letter to new employer and employee with reminder of continuing obligations
- Consider preserving departing employee's emails and/or forensically imaging electronic devices
- Consider using an exit interview certification

# Need for Litigation

- Do you have people in place to collect devices?
  - Do you have ability to get devices to forensic investigators?
- Do you have access to documents/agreements necessary to file?
- Will court hear motion?
  - Under circumstances, you may have to assume it will not
  - Unless demonstrable, serious emergency
- Can motion/filing wait? Other means to address issue? Letter writing? Agreement to sideline with other business?

# Policy v. Protection



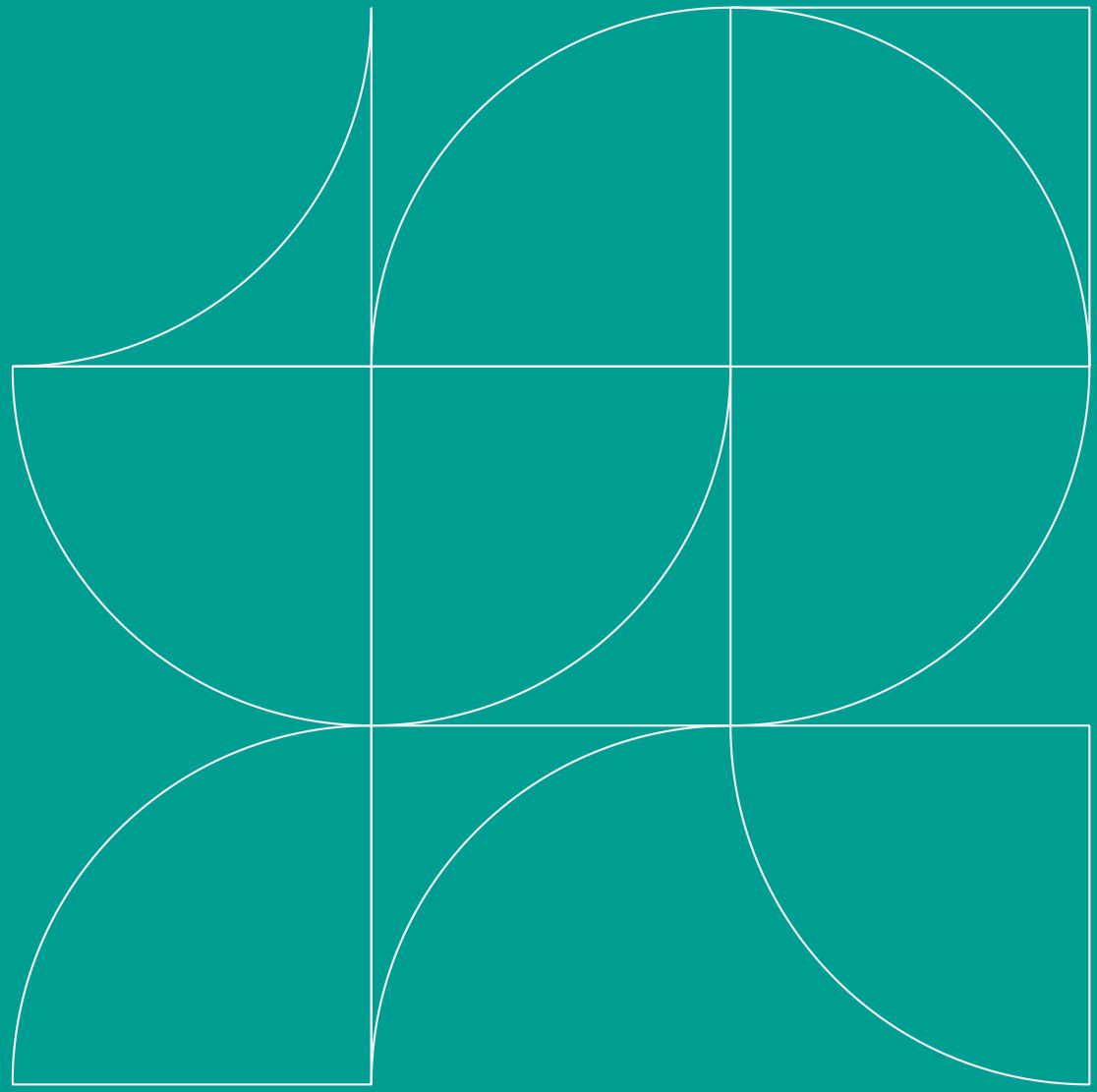
# Electronic Security

- Knowledge of current technology (and accompanying risks) and computer forensics is essential.
- Risks:
  - Employees can use flash drives and personal e-mail accounts to electronically transmit documents containing trade secrets.
  - Employees can use personal devices such as cell phone cameras, iPhones, and portable music players to capture data.
  - Can leak information using social networking sites and other Internet forums.
  - Failure to install extra levels of security may be used by courts as an indication of a company's failure to take reasonable measures to maintain secrecy.

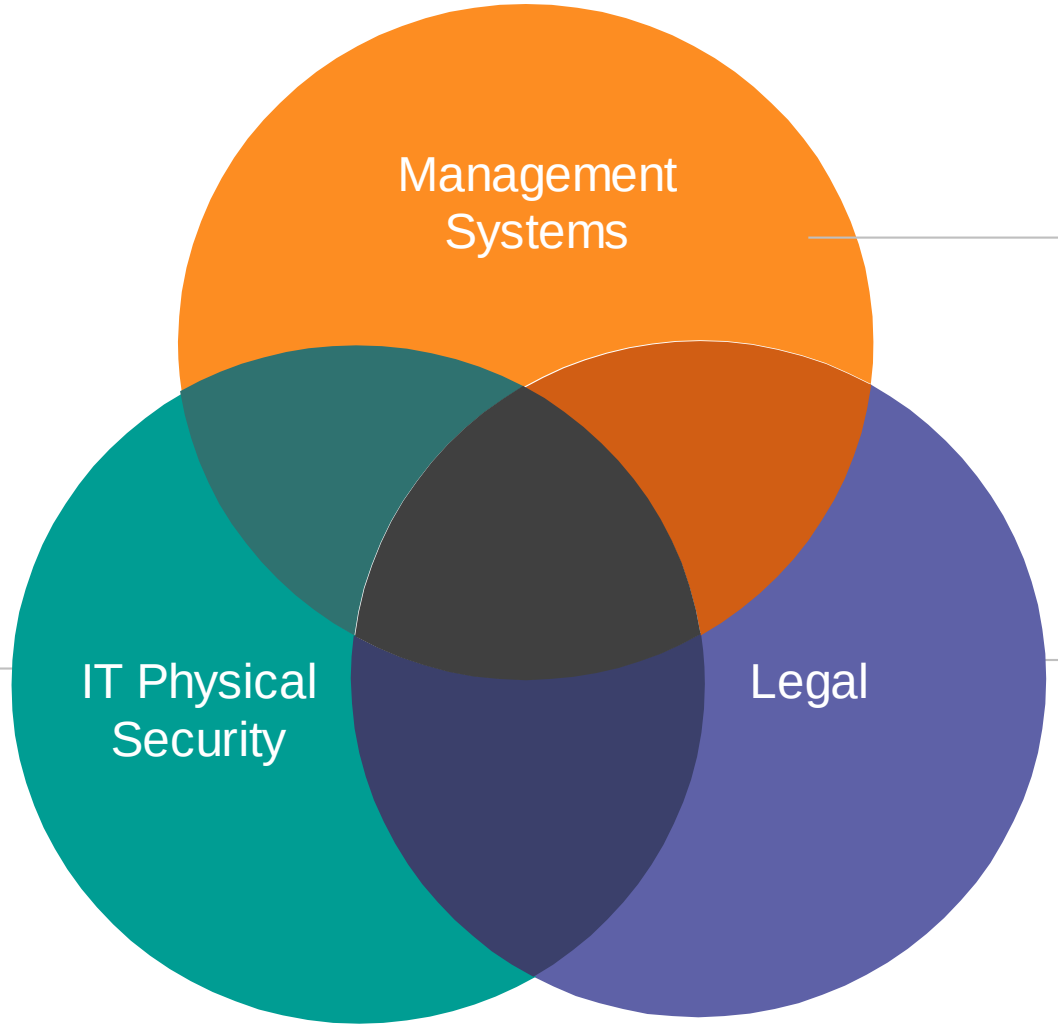
## **Ownership of Data**/Continuity of Access to Data

- Designate Ownership of Information
- Survival Provisions
- Diversification of Data Centers and Back-up Plan
- Avoid Withholding of Data for Failure to Pay
- Assistance for Transitioning and Moving Data to New Provider
- Restrict Use/Sale to Outside Third Parties
- Hold Provider and Subcontractors Liable for Breaches

# What Should You Be Doing Now?



# Pillars of Effective Trade Secret Protection




Trained, committed people routinely following procedures

Access-control, secure networks and facilities, etc.

Contracts & Litigation

# Current Scenarios

- Virtualized Environments
- Laptops Connecting To Corporate VPN
- Home Computers Used For Work

# Issues With Personal Devices

- Data Existing on Personal Devices
- Encryption and Transmission Compromised
- Malware Issues
- Data Location Unknown

# What You Need To Do Now, It's Not Too Late

- Determine if you have a policy, procedure in place.
  - If not, create one.
- Audit/Survey your employees, what are they doing?
- What devices or tools are employees using?
- Where are employees working?
- **Use tools such as Survey Monkey to gather data.**
- Deploy company owned devices and memory tools.
- Sign-In screens are critical, make a change now.
- Issue reminder memorandum to all employees.
- Conduct training webinar call.
- Enforce policies.

# What You Need To Do Now, It's Not Too Late

- Monitor for issues.
- Track access to company data and files.
- Use proper software to prevent malware, phishing and viruses in email and attachments and training.
- Develop plan now for return to normal work patterns and new remote work force displacement.
- Develop plan to ensure return of company information after shelter-in-place ceases.

# Laid-Off and Furloughed Employees

- Copy hard drive and store
- Turn off access
- Exit interview
- Signed certification
- Reminder letter
- Monitor for issues

# Recommendations

## on protecting trade secrets from cybersecurity threats

To guard against cybersecurity threats, employers should consider:

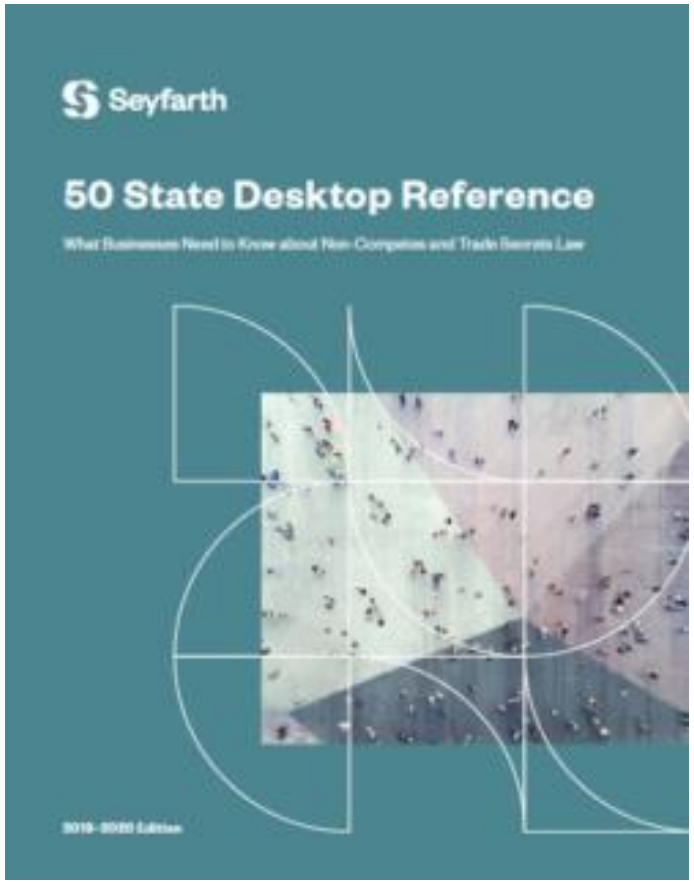
- Require all employee devices to be equipped with the employer-provided security software and the latest manufacturer software updates prior to permitting access to any remote systems;
- Require multifactor authentication upon each login to a company portal;
- Only allow remote access through a virtual private network (VPN) with strong end-to-end encryption;
- Prohibit working from public places, such as coffee shops or on public transportation, where third parties can view screens and printed documents;
- Prohibit use of public WiFi, and require the use of secure, password-protected home WiFi or hotspots; and
- Impose additional credentialing with respect to the ability to download certain sensitive data.

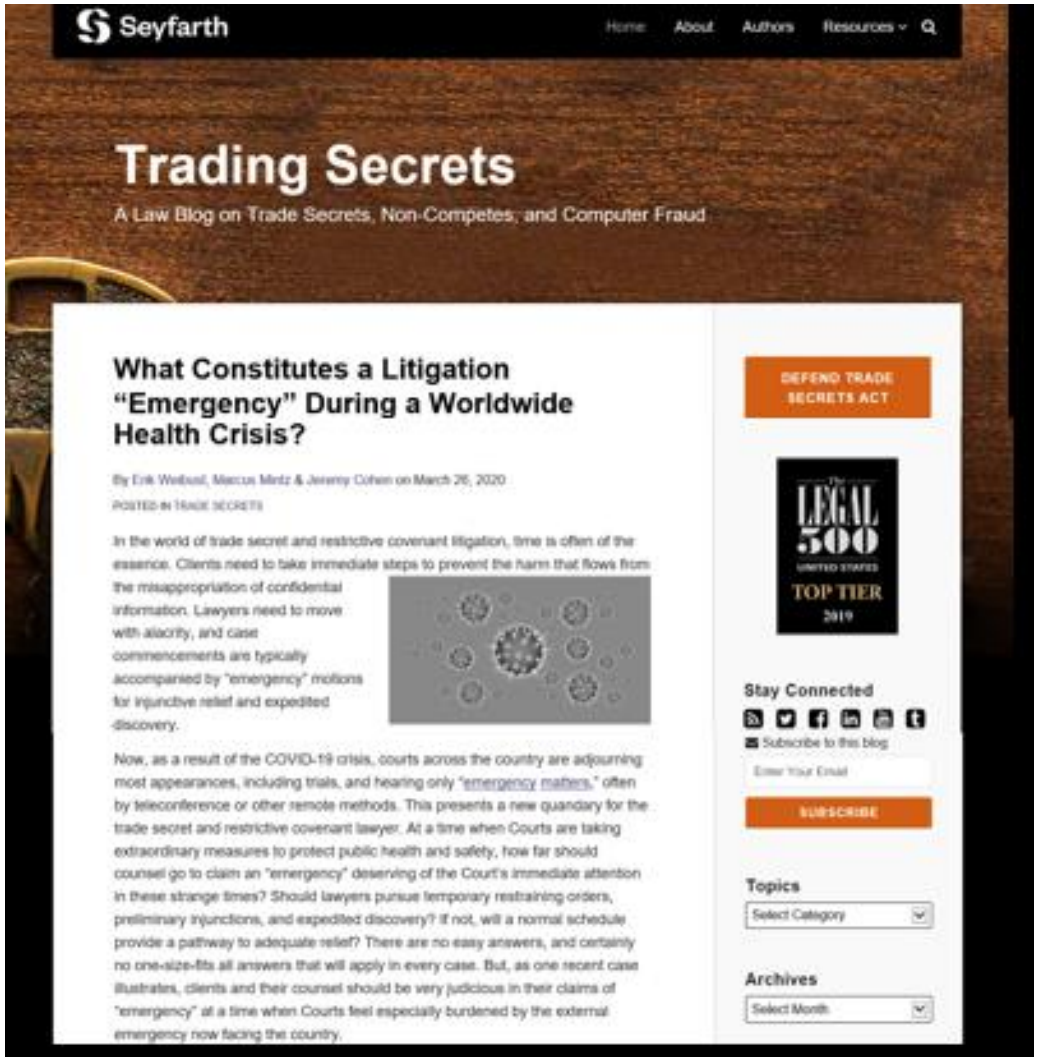
# Additional Recommendations

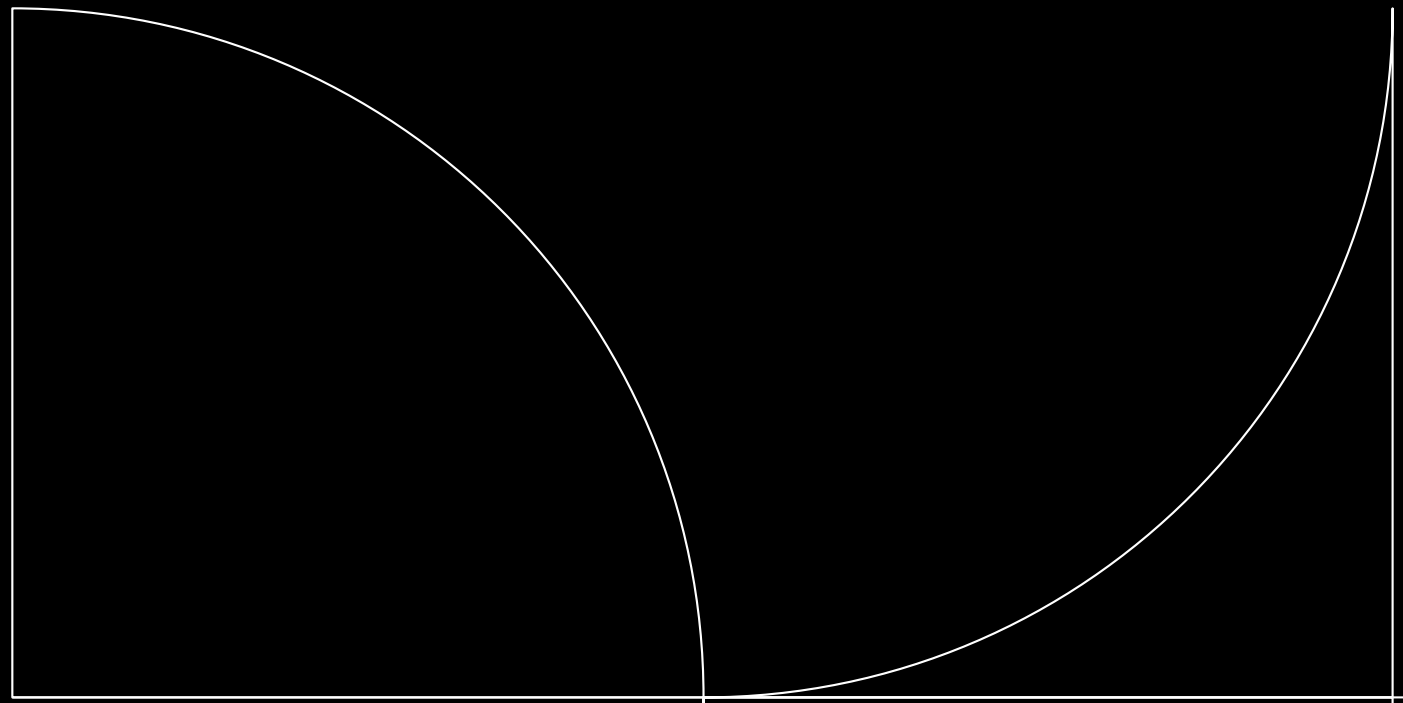
- Set clear expectations with employees
- Engage in immediate training on new policies and procedures
- Monitor your employees and require them to check in
- Take steps now to reinforce your technical security infrastructure
- Require employees working from home to use

# Resources

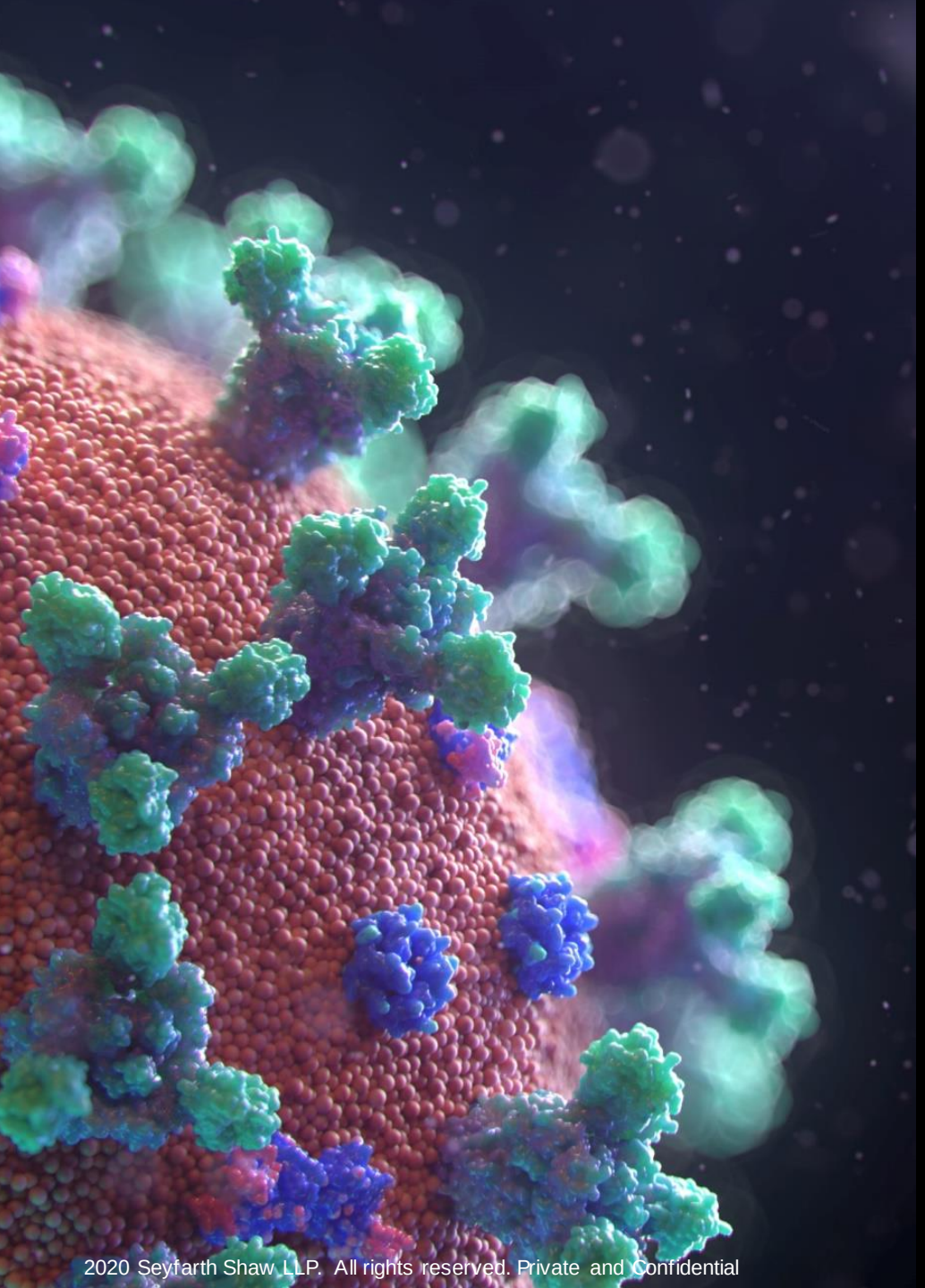
www.tradesecretslaw.com
www.seyfarth.com/covid19



# Questions?



**Visit our COVID-19 Resource Center to sign up for daily updates:**

www.seyfarth.com/covid19