Trade Secret Protection Risk and the Remote Workforce: 10 Questions to Address

Agenda

- **Table Setting**
  - Introductions
  - Historical risk for trade secret protection
  - Current State – the COVID-19 work-from-home environment and its effect on Trade Secret Protection Risk
- **Legal Questions to ask and Recommendations to protect your Trade Secrets**
- **Technology Questions to ask and Recommendations to protect your Trade Secrets**

Panelists

SHANNON MURPHY

PARTNER
Winston & Strawn LLP

MARK CLEWS

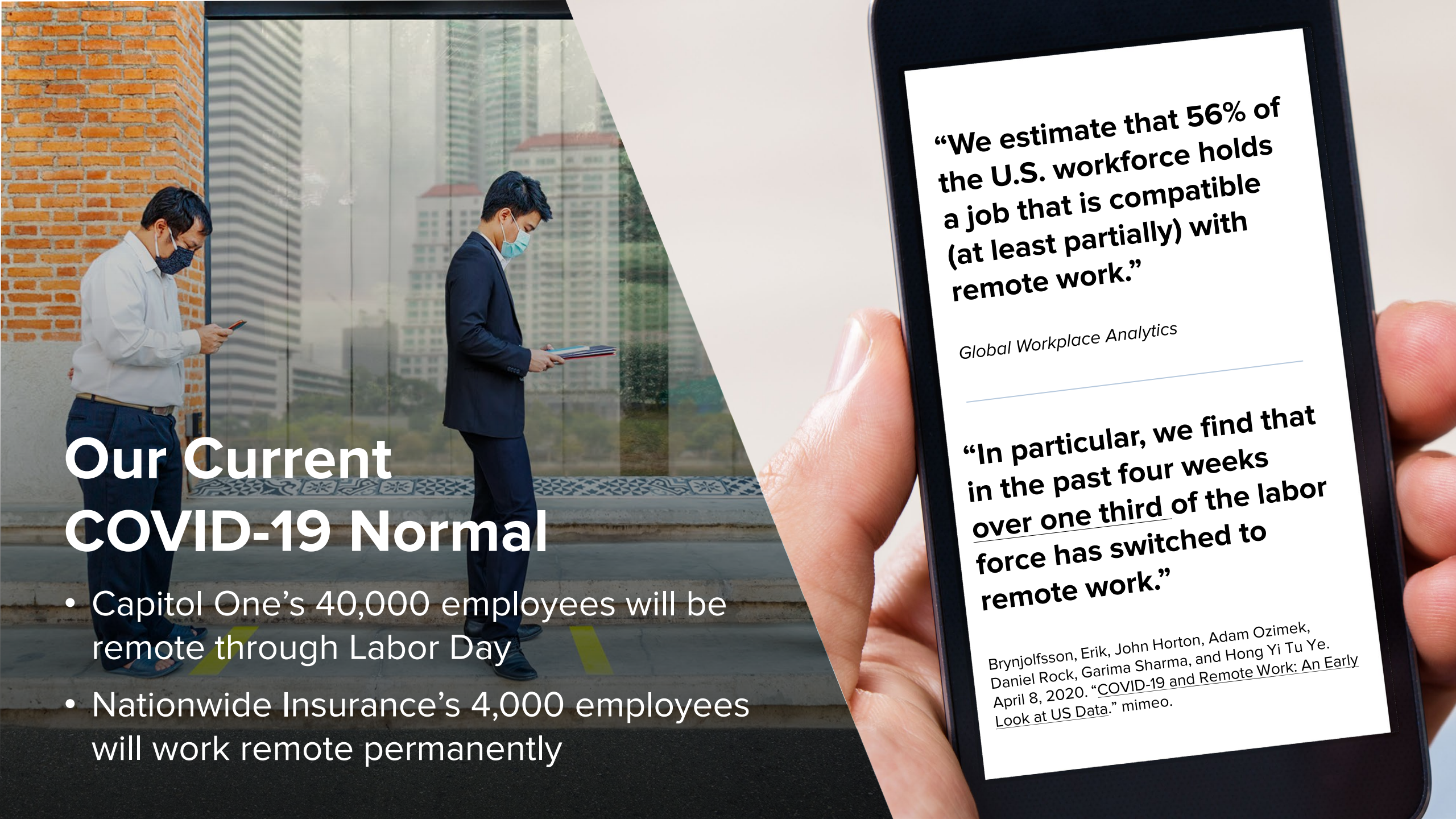
SENIOR MANAGING DIRECTOR
Ankura

LUKE TENERY

SENIOR MANAGING DIRECTOR
Ankura

ankura | WINSTON & STRAWN LLP

Remote Work:
A New Short- and Long-Term Normal



Our Current COVID-19 Normal

- Capitol One's 40,000 employees will be remote through Labor Day
- Nationwide Insurance's 4,000 employees will work remote permanently

"We estimate that 56% of the U.S. workforce holds a job that is compatible (at least partially) with remote work."

Global Workplace Analytics

"In particular, we find that in the past four weeks over one third of the labor force has switched to remote work."

Brynjolfsson, Erik, John Horton, Adam Ozimek, Daniel Rock, Garima Sharma, and Hong Yi Tu Ye. April 8, 2020. "COVID-19 and Remote Work: An Early Look at US Data." mimeo.

COVID-19 could change work settings permanently; COVID-19 has corporations re-thinking working from home

Winston-Salem Journal (North Carolina) – April 26, 2020

Nationwide announces permanent shift in workplace, work-from-home strategy

PR Newswire – April 29, 2020

Twitter says staff can continue working from home permanently.

TechCrunch – May 12, 2020

Michael Dell: Work From Home Will Be 'Permanent Feature'

CRN.com – May 12, 2020

WFH may Find Permanent Home in IT Contracts

Economic Times (E-Paper Edition)

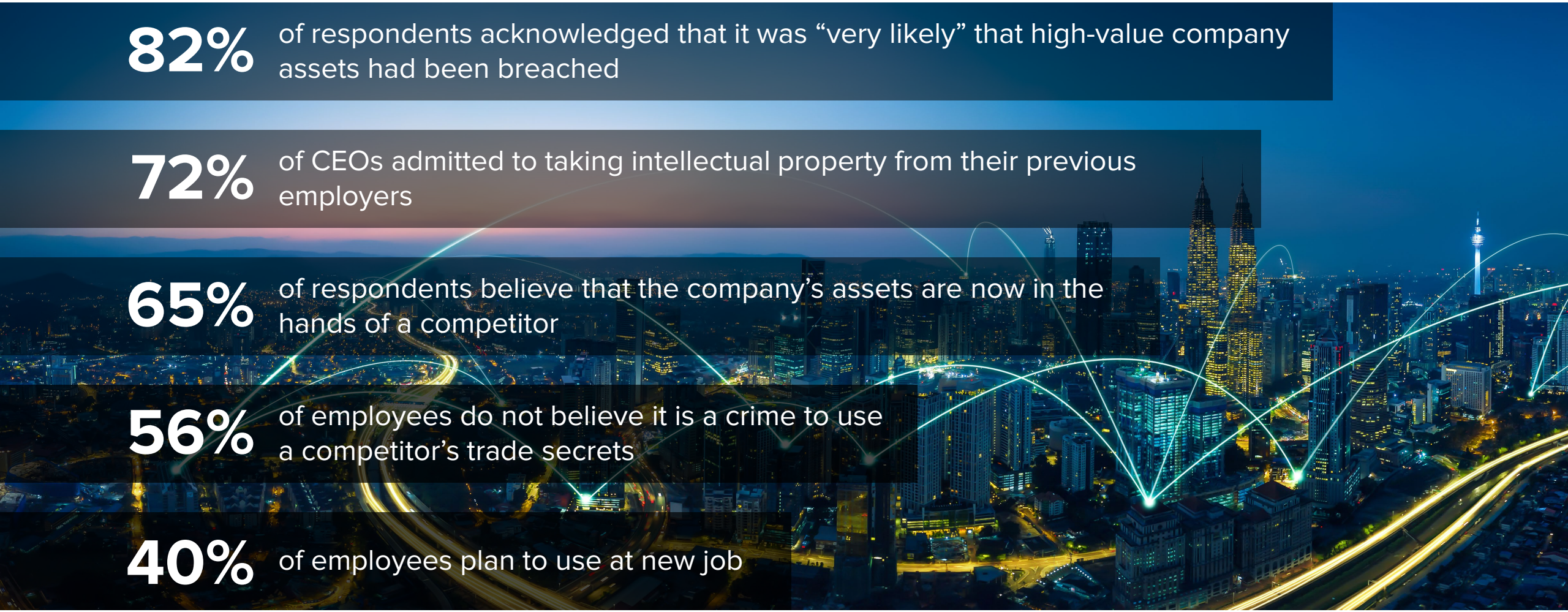
The New/Permanent COVID-19 Normal

- Gartner CFO Survey Reveals 74% Intend to Shift Some Employees to Remote Work Permanently
- Arlington, VA, April 3, 2020

ankura | WINSTON & STRAWN LLP

The Risk to Trade Secret Protection

Employees Always Pose a Risk



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

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

65% of respondents believe that the company’s assets are now in the hands of a competitor

56% 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

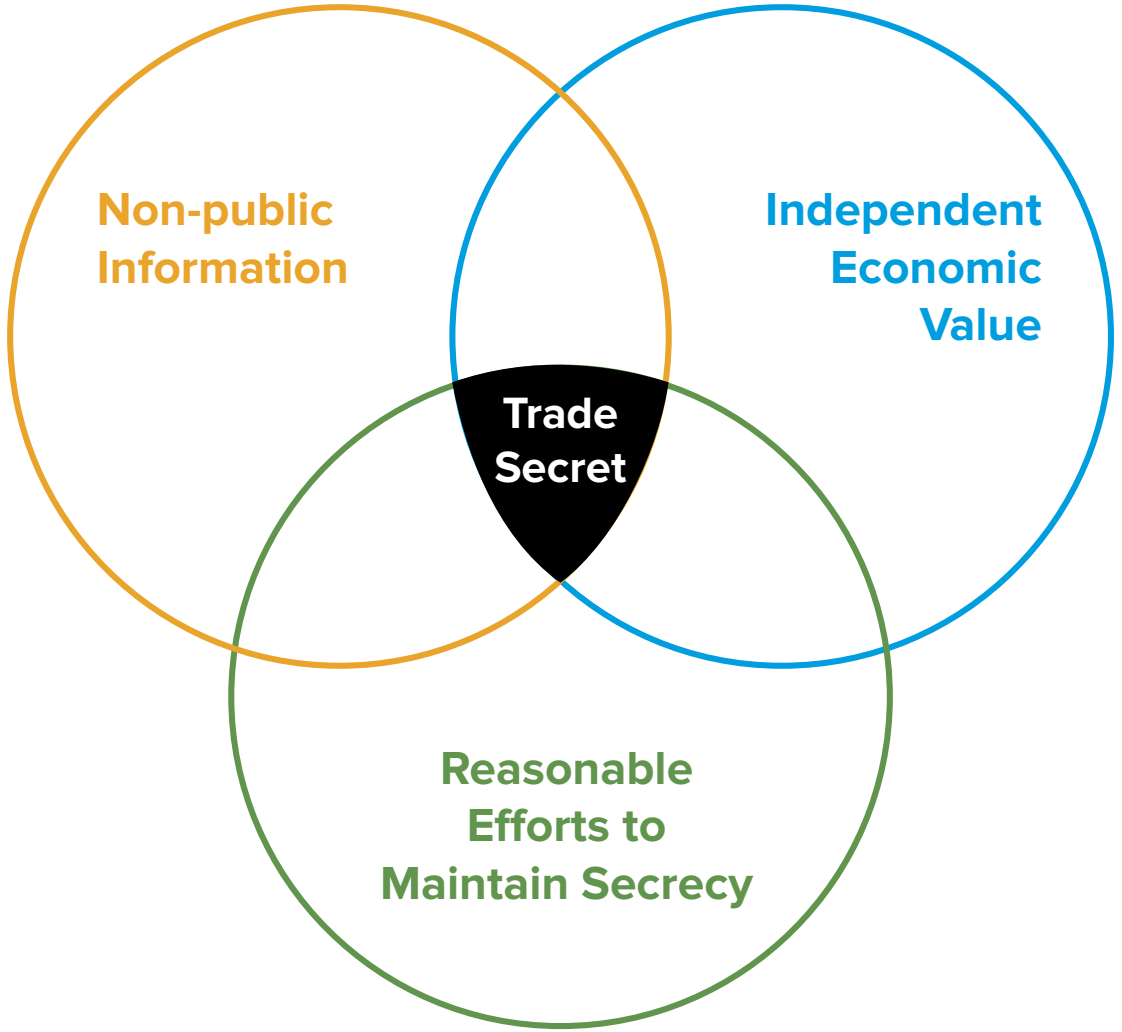
Risk of Employee Theft Is Particularly High

- 2007–2009 recession: DOW decrease of 50%, 37 million unemployment claims
  - Increased employee mobility
  - Increased trade secret cases in following 5 years
- COVID impact → decreases in DOW and millions of unemployment claims
  - Prediction: increase in trade secret claims

Ripe for Outsider Attacks

- Current COVID-19 climate has changed IT landscape of many companies
- Majority of employees often no longer within secure walls of the company
- Rapid deployment of WFH has left holes in IT security
- Phishing emails related to COVID-19 on the rise

Risk Permanent Loss of Protection as a Trade Secret



May Not Be Prepared for Evidence Collection

- WFH employees may use personal devices and/or unsanctioned tools to conduct their work
- Challenging to identify devices and data sources for preservation
- Logistical challenges in preserving WFH assets
- Redundancy measures are often lacking in home office setups
- Missing key data sources can result in spoliation claims

Trade Secret Damage Is Significant

Various Types of Harm/Costs

Reputational Costs	**Loss of Competitive Advantage**	**Investigation/ Disruption Costs**	**Uncertainty**

ankura | WINSTON & STRAWN LLP

10 Questions to Ask to Ensure Your Company's Secrets Are Protected

Question 1:

Do employees understand what constitutes a “trade secret”?

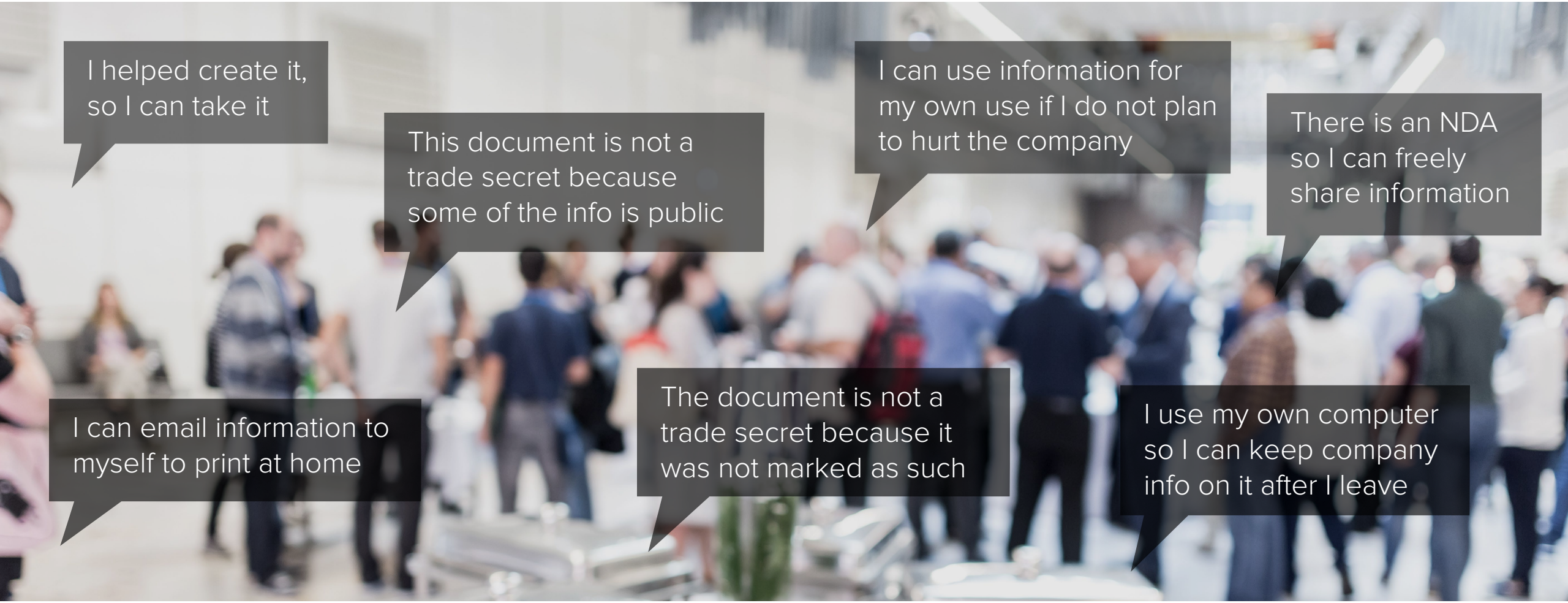
Issue:

- Employees are on the front line of trade secret protection
- Crucial that they understand what constitutes a trade secret and the importance of protecting that information
- If employees do not understand that something is a trade secret, they may fail to protect that information

Issue:

- What constitutes a “trade secret” is a legal question – and what qualifies is much broader than most employees realize
- Secret formulas and schematics are the obvious trade secrets… but this is just a subset of the full breadth of information that can be protected
  - Negative trade secrets – failed trials or earlier versions
  - Combination trade secrets – all of the information can be publicly available, but the combination can make it a trade secret

Common Employee Misconceptions



Practical Guidance:

- Companies should implement a robust, learning-based training program regarding trade secrets
  - Education – not just check-the-box training
- Avoid boilerplate language when describing confidential information
  - An employee should be able to understand what constitutes a trade secret
- Create a stand-alone trade secret policy including information on:
  - IP ownership
  - Indemnification
  - Cooperating obligation
  - Confidentiality
  - No expectation of privacy
  - Acceptable IT and email use

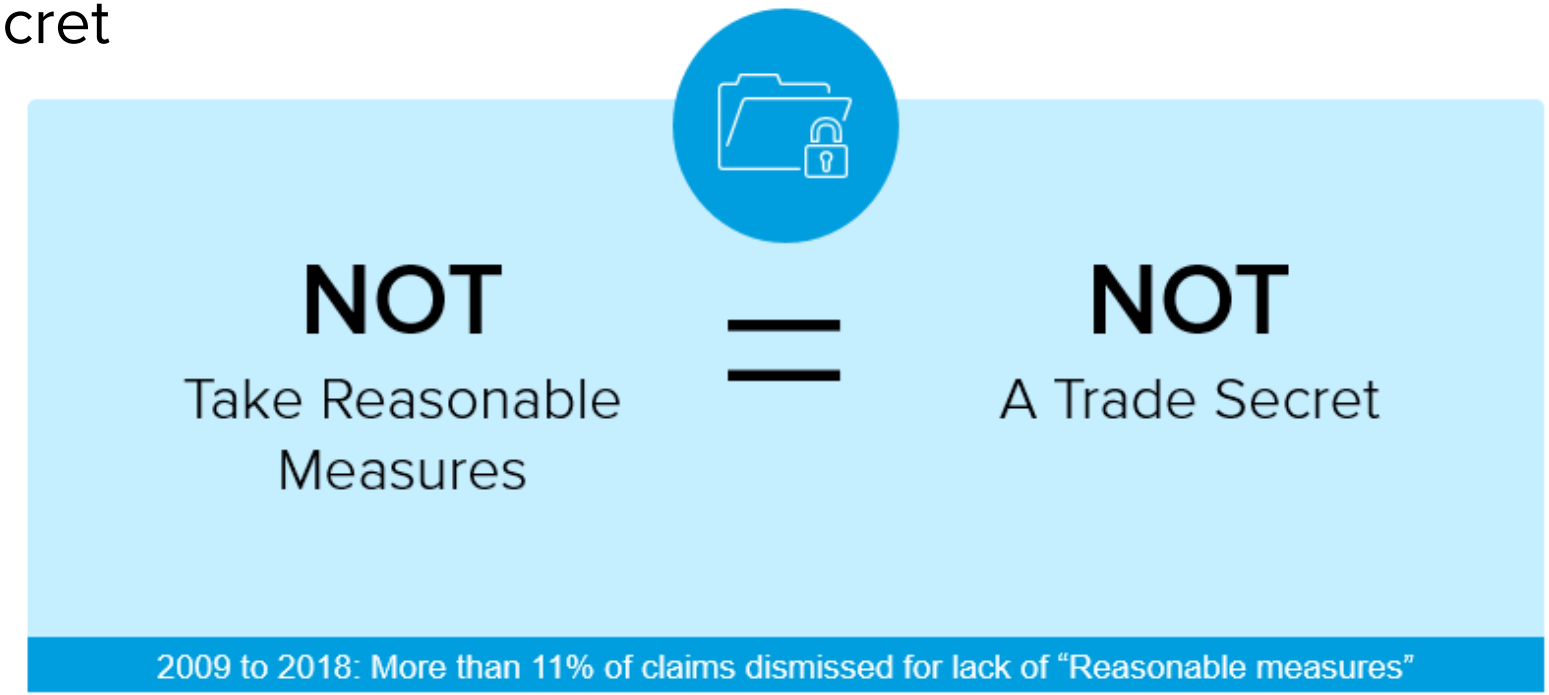
ankura | WINSTON & STRAWN LLP

Question 2:

Is access to information being limited on a need-to-know basis?

Issue:

- Trade secret laws require that a trade secret owner take **reasonable measures** to protect information in order for that information to qualify as a trade secret



- One of the key measures courts look at is whether the company limited access to the information on a **need-to-know basis**

Practical Guidance:

- Implement written policies that instruct employees to limit access to confidential information to a need-to-know basis
  - Employees should have a demonstrated need for access to the information
- Utilize IT policies to limit access on file, application, or database level
- Audit access rights
  - Access to data should be regularly monitored and updated as employees shift roles or otherwise no longer need access to confidential information
  - Future data breaches can expose credentials of stale user accounts

Practical Guidance cont:

- Cloud Security Alliance (CSA) organization helps to identify and disseminate best practices for securing cloud infrastructure
- Cloud solutions provide Identity and Access Management (IAM) for granular control over user permissions
- Leverage Privileged Identity Management (PIM) to further limit time/scope of admin actions
  - Example: Grant user X admin rights to perform action Y; admin rights to expire in 4 hours
- Cloud solutions can provide escalation flows that leverage PIM or other cloud-based IAM controls to temporarily grant access
- Routinely audit and disable stale accounts, especially admin accounts

Question 3:

Are employees re-certifying understanding of compliance with relevant policies?

Issue:

- The reality is that employees do not often have confidentiality and compliance policies at front of mind – they need reminders
- Often times, these policies are addressed only at the start of employment, and then forgotten by employees
- Increased risks created by remote work make these security and confidentiality policies that much more important

Practical Guidance:

- Now + periodically: remind employees of their obligations
  - Send updated trainings or security-related newsletters or other reminders
- Conduct updated trainings on security and confidentiality obligations
- Consider re-certification of continued compliance
  - Even better: annual re-certification procedures
- Two benefits:
  - Increase compliance + provide legal support for future lawsuit

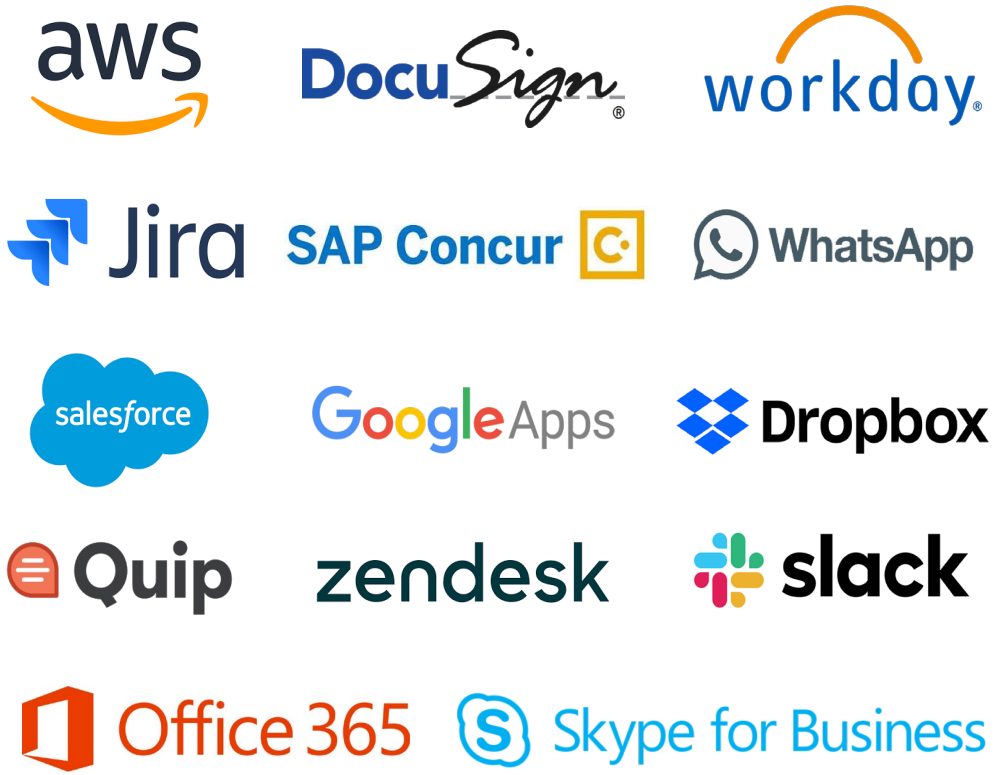
Question 4:

Are employees using free cloud-based storage or cloud-based collaboration tools?

Issue:

- Core concern: Employees will find a way to make their job easier and more efficient
  - If a business does not provide secure and efficient solutions employees will circumvent this by signing up for free versions of a tool and conduct business on unapproved platforms
- Often free SaaS solutions mine data for advertising purposes
- Many free SaaS solutions do not have legal hold or eDiscovery utilities to preserve the data in a defensible manner

COMMON CLOUD PLATFORMS & APPLICATIONS



Practical Guidance:

- Educate employees of the risks of using these free cloud platforms for corporate purposes

- Understand what your employees are using these platforms for and provide secure, corporate approved solutions

Question 5:

Are employees using non-secure, non-sanctioned communications and collaboration platforms?

Issue:

- With the explosive spike in employees WFH, video conferencing has skyrocketed
- If the employer does not have a video conferencing solution, or one that is not as easy to use for their employees, they may be using unapproved, free-to-use products
- If not implemented securely, unauthorized access is possible by bad actors
- If a secure, company-approved solution is provided, bad security habits by hosts can expose the company to the risk of IP theft

Practical Guidance:

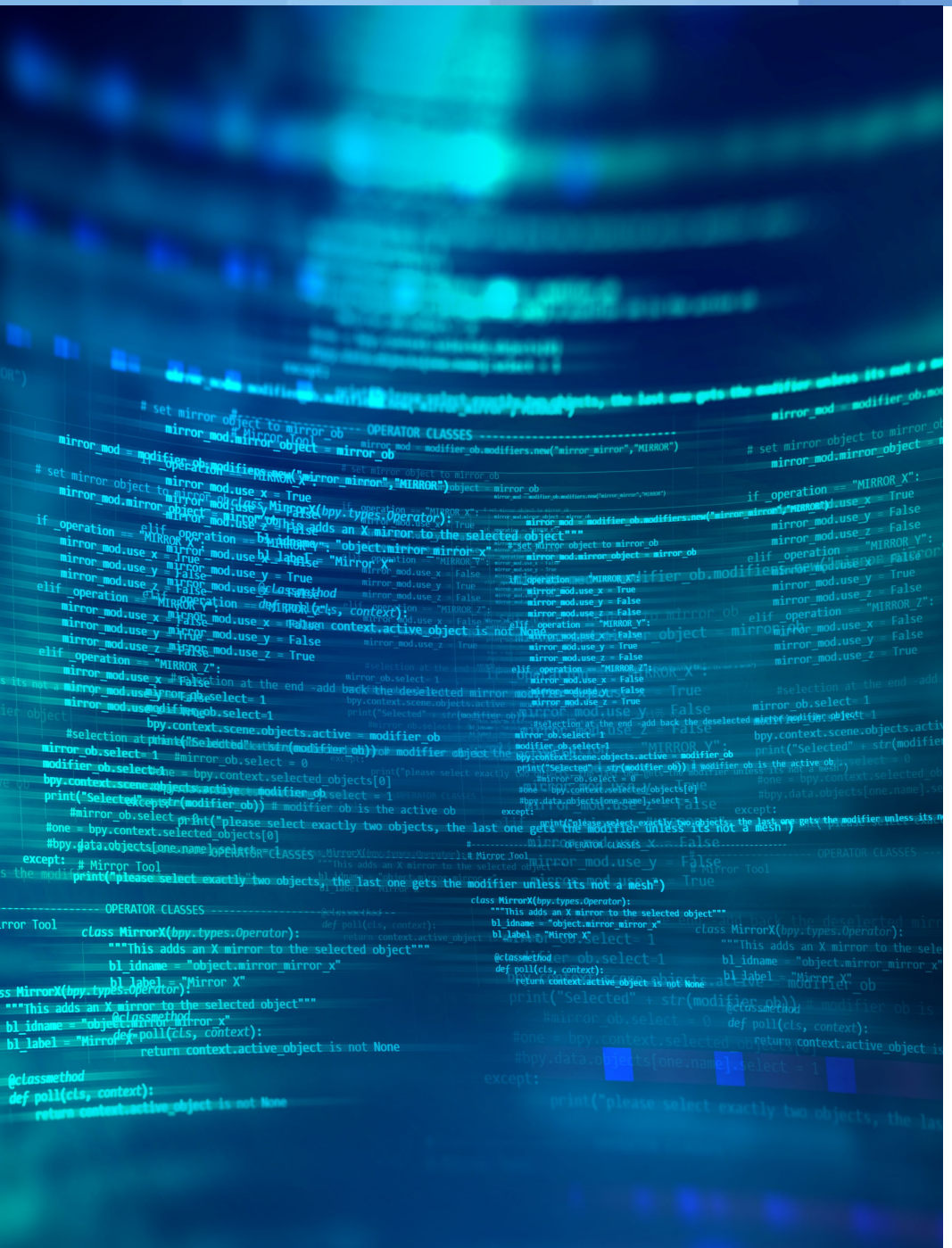
- Educate your employees to the dangers of using free, unsecured communication solutions
- Provide a communication platform that has default security settings, for example:
  - Entrance passwords required
  - Repeatable meetings should change IDs and passwords
  - Enable waiting rooms
  - Granular control over meeting participants (remove, disable private chat, etc.)
- Shutting down accounts of former employees as part of their offboarding
- Consider shutting down access to furloughed employees
- Consider the settings to reduce risk, i.e., configure the communication platform to not retain chat logs

Question 6:

Are employees sharing data with third parties in a responsible and protected way?

Issue:

- Employers often default to using email or cloud-based sharing platforms
  - May increase/seem more convenient with WFH
- Dangerous misconception: non-disclosure agreement is sufficient
- Need to maintain control over data + limit access and dissemination by third parties
- Employees will find problematic workarounds (e.g. Dropbox)



Practical Guidance:

- Ensure clearly articulated protocols are in place for third-party sharing
  - Policies should include which tools are to be used for such sharing, and employees should be educated on how to use these tools
  - There must be a viable option!
- Use secure transfer methods (FTP), limit downloads, and set an expiration date for file access

Practical Guidance:

- Block disallowed transfer mechanisms (for example, set internal controls so that employees cannot download applications that are not company-approved)
- Consider solutions such as AppLocker for whitelisting apps that can be downloaded/installed on endpoints
- Leverage API of SaaS solutions to monitor file sharing with external users, downloads, etc.

ankura | WINSTON & STRAWN LLP

Question 7:

Do security policies protect data from outside and internal threats?

Issue:

- Security policies inform expectations, but technical controls are needed to ensure compliance
  - Example: MFA requirement in policy v. technical requirement
- Outside threats and rogue insiders don’t care about security policies
- Technical controls can be used to audit compliance with security policy

Practical Guidance:

- Policies without governance can be problematic
- Ensure that security policies are supported by controls to enforce compliance
- Examples of technical controls:
  - Limit sign-ins to specific IP(s)
  - Block sign-ins from anonymous IPs
  - Configure firewall rules to mitigate unauthorized access
  - Configure audit and alerting notifications when specific conditions are met
- Services such as Microsoft Azure AD Identity Protection can streamline much of this

ankura | WINSTON & STRAWN LLP

Question 8:

Are hard-copy or tangible trade secrets protected from employees' roommates?

Issue:

- Many employees are now sharing their working space with others
  - Roommates
  - Family
  - Visitors

  * Even possible that an employee lives with a roommate working for a rival company

- Data on screens, printed, or left in the open poses risk

Practical Guidance:

- Create or update a “clean desk” policy
- Account for WFH scenarios by:
  - Discouraging employees from printing confidential or trade secret documents
  - Providing instructions for destruction of such materials
  - Directing employees re secure storage for tangible company material
- Consider providing remote workers with equipment (shredders) to facilitate destruction of sensitive information

Question 9:

Are devices being collected or wiped promptly (ideally before termination) in all cases?

Issue:

- When an employee resigns or is terminated, it is critical to collect devices and terminate access to company data ASAP
- Remote work creates added logistical difficulties for such collection
- More personal devices may be implicated
  - Must beware of consent + privacy issues
- But these rapid collection, wiping, and access termination efforts are crucial to both:
  - (1) minimize the chance of theft; and
  - (2) increase the chance of emergency relief, if a theft does occur

Practical Guidance:

- With input from HR, IT, and business managers, create a plan to ensure prompt device collection
- If possible, the company should implement a process to collect devices prior to termination
  - For example, IT could request return of the company devices for routine maintenance prior to termination
- Require immediate return of company devices and engage in persistent follow-up until the device is returned
- Probe what employees' use of data has been
- Look at logs to identify devices used
- Document company efforts to collect devices

ankura | WINSTON & STRAWN LLP

Question 10:

Do applications provide sufficient visibility to detect cyber threats and insider theft?

Issue:

- IT infrastructure is increasingly being moved to the Cloud
  - Email: Microsoft 365, G-Suite
  - Document Storage: OneDrive, Dropbox, Google Drive
  - Computing: AWS Elastic Compute Cloud (EC2), Microsoft Azure VMs
- Governing Cloud resources has been a growing problem
- Requirement for visibility into an identity has dramatically increased with Cloud adoption
  - Example: How do we identify suspicious access from a user account?

Practical Guidance:

- Some SaaS platforms are better than others in providing visibility
- We often don't know what we don't know – requires study of your individual organization
- Different from platform to platform
- Relying on identity access management and least privilege principles – more fashionably Zero Trust – is a more reasonable solution
- Solutions exist to leverage APIs provided by SaaS platforms to aggregate logs and improve visibility across multiple SaaS products
  - Must ensure appropriate logging is enabled
- Other Questions to Ask:
  - Do I have controls in place to detect potentially harmful behavior? E.g., mass file downloads or publicly available files?

Proactive Approach to Trade Secrets

Two Goals
minimizing theft +
increasing legal options

Thank you

SHANNON MURPHY

PARTNER
Winston & Strawn LLP

MARK CLEWS

SENIOR MANAGING DIRECTOR
Ankura

LUKE TENERY

SENIOR MANAGING DIRECTOR
Ankura

