Russell Beck
Beck Reed Riden LLP
rbeck@beckreed.com

A PRIMER AND CHECKLIST FOR PROTECTING TRADE SECRETS AND OTHER LEGITIMATE BUSINESS INTERESTS

Hope for the best, plan for the worst.
- John Jay[1]

The ability to protect trade secrets (and other legitimate business interests, including other confidential information and customer goodwill) is a difficult task that requires planning and dedication, even in the best of circumstances. There are many reasons for that, including the following:

- **Risk of Theft**. According to at least one survey of workers, 59 percent of employees *admit* that they took confidential information with them when they left their job.[2] But "[n]ot every insider risk becomes an insider threat . . . ."[3] Oftentimes workers engage in this conduct not because they want to harm their soon-to-be former employer, but rather because they believe they have a right to retain information, especially if they participated in creating the information.[4]
- **Lack of Control**. With any part of a workforce working remotely, it can be especially difficult to ensure that trade secrets (as well as customer relationships and other legitimate business interests) are properly protected.
- **Loss of Protections**. In many states, employees who have been laid off without cause are relieved of their noncompete obligations, even though

[1] *See The Correspondence and Public Papers of John Jay, vol. 4 (1794-1826)*, available at https://oll.libertyfund.org/title/johnston-the-correspondence-and-public-papers-of-john-jay-vol-4-1794-1826.

[2] *See Survey: 59 percent of fired workers steal data on way out*, available at https://www.computerworld.com/article/2770778/survey--59-percent-of-fired-workers-steal-data-on-way-out.html.

[3] *The Cost of Insider Threats*, available at https://www2.dtexsystems.com/l/464342/2023-09-15/3w7l7k/464342/1694800570ZwvyrzsD/2023_Cost_of_Insider_Risks_Global_Report___Ponemon_and_DTEX___Dgtl.pdf ("Not every insider risk becomes an insider threat; however, every insider threat started as an insider risk," *quoting* Gartner).

[4] *Symantec Study Shows Employees Steal Corporate Data and Don't Believe It's Wrong*, available at https://finance.yahoo.com/news/symantec-study-shows-employees-steal-130000357.html; *see also The Cost of Insider Threats*, *supra* n.3 ("Non-malicious insiders accounted for 75% of incidents, from either: negligent or mistaken insiders (55%), or outsmarted insiders who were exploited by an external attack or adversary (20%). While malicious insider incidents were less frequent (25%) . . . .").

subsequent employment may place their former employer's trade secrets, customer relationships, and other legitimate business interests at risk.[5]

- **Increased Skepticism**. Over the years, courts have become more sophisticated and therefore demanding when asked to issue temporary restraining orders, preliminary injunctions, and similar emergency orders (critical relief often necessary to protect trade secrets and other legitimate business interests).
- **Threats to the Use of Safeguards**. As we look forward, there are increasing state and federal efforts to remove critical tools needed to protect trade secrets.[6]

While we can certainly hope that everyone will be careful, diligent, and comply with their legal obligations, we need to plan for the opposite.

Accordingly, below is **practical guidance** for companies to follow to protect their trade secrets (and other legitimate business interests) – both generally and especially if they employ a remote (or hybrid-remote) workforce. By following the guidance and having a plan in place to address problems when they arise, which they inevitably will, companies will stand a much better chance of successfully preventing preventable problems. Accordingly, below is an **explanation of the general elements** of a trade secret protection program, **a detailed guide** to the creation of a trade secret protection program, and **the tools needed to identify where to focus efforts**.

AN OUNCE OF PREVENTION

I have always been a believer that when it comes to the protection of trade secrets (and other legitimate business interests), an ounce of prevention is worth a pound of cure. That is even more true now. The current circumstances mandate increased vigilance – but, increased vigilance tempered by reality.

In words of warning as applicable now as they were during the Covid-19 pandemic, Jim Pooley wisely cautioned[7]:

> During this unusual time, employers need to be flexible and understanding. Getting compliance with the full suite of security protocols is harder at a distance. Trade secret management is about balancing value against risk, and then measuring that risk against the cost (including inconvenience) of various

[5] To see which states, see the chart available at https://www.beckreedriden.com/50-state-noncompete-chart-2/.

[6] *See Noncompetes, the sky is not falling*, available at https://faircompetitionlaw.com/2023/09/18/noncompetes-the-sky-is-not-falling/.

[7] *See Do Your 'Home Work': Keeping Trade Secrets Safe While Working Remotely*, available at https://www.ipwatchdog.com/2020/03/26/homework-keeping-trade-secrets-safe-working-remotely/id=120185/.

> measures to reduce it. One of the practical risks is that people won't follow rules that get in the way of getting the job done, and so you need to be sensitive to their struggle and try to collaborate about finding acceptable solutions.

The important thing to remember is that the rules and circumstances have only gotten more demanding in recent years. Accordingly, it is critical to have a working trade secret protection program[8] that reflects the current realities.

A Proper Trade Secret Protection Program Explained

At its core, a trade secret protection program is a set of protocols to protect a company's confidential information – protocols that are not only expected by courts, but, more important, protocols that are designed to prevent the misappropriation of a company's information in the first place.

While "reasonable" efforts are the legal touchstone for protecting trade secrets, the law should not be the motivation. Rather, effective and efficient prevention of misappropriation should be the lodestar.

Few trade secrets are like Coca-Cola, requiring heroic measures for their protection.[9] In most instances, companies can achieve a reasonable balance, preventing misappropriation while enabling employees to use the company's information for legitimate business purposes. The goal should be to ensure that protecting the information is the easy path. If the balance tips too far toward preventing misappropriation, making it difficult for employees to get their work done efficiently, they will find a workaround. In contrast, the less resistance, the more likely compliance will happen naturally.

Over a decade ago I wrote, *The Who, What, Where, When, How, and Why of Trade Secret Audits*,[10] providing an overview of how to do this. The process remains the same. But, like everything else, shifting paradigms require recalibrating tools. What is reasonable today is qualitatively different from what was reasonable in the past. What worked for a physical Rolodex had to be recalibrated for iPhone contacts, LinkedIn, and other social media. And what worked with a predominantly local workforce may no longer work in a world with a workforce that involves remote work.

---

[8] While discussed in terms of trade secrets, such a program is more expansive, and consideration should be given to steps to protect other legitimate business interests (such as other types of confidential information, customer goodwill, and the integrity of the company's workforce).

[9] *Coca-Cola's formula is not really so much of a secret that only two men each know half of it*, https://www.snopes.com/fact-check/coca-cola-fomula/?collection-id=209643.

[10] Available at https://www.faircompetitionlaw.com/2010/07/04/the-who-what-where-when-how-and-why-of-trade-secret-audits/.

There is no one size fits all approach. The reasonableness – and effectiveness – of the protection measures will depend on the nature of the information, the value of the information, the potential risks to the information, and the circumstances of the company.

A Checklist for Trade Secret Protection

Set forth below are the steps – together with a checklist of questions and protections – for a proper trade secret protection program ("TSPP").

Remember that companies, their culture and circumstances, the nature of their trade secrets and other confidential information, and the risks they face vary widely and will require different approaches – and they all change over time. What may have made sense at one time may no longer be sufficient or may be too restrictive. So this process should be considered a work-in-progress, to be reevaluated on a regular basis.

Also note that this checklist does not address the requirements imposed by potentially applicable regulatory overlays such as HIPAA or Reg S-P. Accordingly, the checklist is necessarily general and must be tailored to the specific circumstances.

Step One: Understand the Landscape

The starting point for protecting trade secrets (and other company information) is gaining an understanding the landscape: What information is at risk and where do the risks come from?

There is an endless variety of trade secrets and confidential information. They can include product developments; specifications or plans for new, revised, or existing products; technical data; designs; patterns; formulas; computer programs; source code; object code; algorithms; subroutines; manuals; products; business plans; business strategies; financial information; customer lists; summaries of customer interactions; customer needs, preferences, and buying patterns; client credit profiles; contract pipeline and opportunities; pending projects and bids; bidding strategies; contracting strategies; marketing and sales strategies; pricing strategies; profitability targets; profit margins; markup rates; price lists; employee lists; vendor information; and so on.

Companies should identify, understand, and categorize their information, not catalogue it. And, depending on the organization, this inquiry may require the involvement of management, human resources, legal, corporate governance, sales, marketing, information technology, information management, research and development, manufacturing, and other relevant stakeholders.

- ❑ **What are the company's trade secrets (*i.e.*, what information is important to company)?**
  - ❑ Does the company own the information?
    - ❑ Who created or developed it?
    - ❑ How was it created or developed?
    - ❑ Does it incorporate anyone else's information?

- ❑ If so, does the company have the right to use that information?
  - ❑ If not, are there corrective measures that must be taken and what rights does the company have?
- ❑ Is the information secret?
- ❑ Does the information have value, whether now or in the future?
  - ❑ How is it valuable?
    - ❑ How long will it remain valuable?
      - ❑ Will it become stale?
- ❑ How widely is the information known in the company?
  - ❑ Is everyone who knows it bound by a nondisclosure agreement ("NDA")?
- ❑ How widely is the information known outside the company?
  - ❑ Is the information generally known in the industry?
  - ❑ Who knows it?
    - ❑ How did they learn it?
    - ❑ Are they bound by confidentiality obligations?
- ❑ How much money and effort did the company expend in developing the information?
- ❑ How easy would it be to recreate the information?
  - ❑ Is it readily ascertainable from public sources or otherwise?
  - ❑ Can it be reverse engineered?
    - ❑ If so, how easily?
- ❑ Is there a process to identify trade secrets on an ongoing basis?
  - ❑ Should there be?

❑ **How are the company's trade secrets protected?**

- ❑ Where are the company's trade secrets kept?
  - ❑ Where are the physical locations?
  - ❑ Where are the electronic locations?
  - ❑ Are any maintained offsite in third-party locations?
- ❑ Who has access to the trade secrets?
  - ❑ Does access vary by employee or category of employee?
  - ❑ Is access limited to those with a need to know?
- ❑ Which of the following is permitted with respect to the trade secrets?
  - ❑ Copying/downloading?
  - ❑ Sharing?
    - ❑ Is sharing tracked?
      - ❑ Are copies retrieved when the purpose of the sharing is satisfied?
  - ❑ Printing?
    - ❑ Are printouts required to be numbered or otherwise controlled?
  - ❑ Taking of screenshot?
  - ❑ Photographing?
  - ❑ Emailing?
  - ❑ Removing the information from the premises?
  - ❑ Does each permitted activity appropriately balance convenience and security?

- ❑ Under what circumstances is each permitted?
- ❑ What are the procedures for doing so?
- ❑ Are controls used (such as check-in/check-out procedures)?

- ❑ Are the trade secrets marked as confidential?
  - ❑ If physical, is the document marked confidential?
  - ❑ If electronic, is "confidential" (or words to that effect) in the document name?
    - ❑ Is there a legend in the document indicating that it is confidential?
  - ❑ Are documents routinely marked confidential, without regard to whether they are in fact confidential? (This should be avoided.)
- ❑ Are the trade secrets secure?

- ❑ **What are the highest value trade secrets or greatest vulnerabilities?**
  - ❑ Are there additional protections?
- ❑ **Are there appropriate backups in case of loss?**
  - ❑ Where are the backups located?
    - ❑ Are applicable policies followed?
- ❑ **Are any trade secrets shared with third parties?**
  - ❑ Which trade secrets are shared?
  - ❑ What are the third parties' obligations for protecting the information?
    - ❑ Is there any reason to doubt the third party's compliance?
    - ❑ Does the company have the right to audit the third party's compliance?
      - ❑ Has the company audited compliance?
  - ❑ What is the third party doing to protect the company's information generally?
  - ❑ What is the third party doing to protect the company's information during the crisis?
    - ❑ Are additional protections needed?
    - ❑ Do specific expectations need to be communicated to the third party?
- ❑ **Which trade secrets belong to third parties?**
  - ❑ What are the company's obligations to the third parties?
    - ❑ Is the company complying with its obligations?
      - ❑ Have there been any changes resulting from the current crisis that affects the company's compliance?

Step Two: Evaluate and Update Protections

Once the landscape is clear, the next step is to evaluate the sufficiency generally and, in particular, from a **physical**, **electronic/technological**, and **administrative** standpoint and then to update the protections, removing anything no longer needed and adding anything missing. The focus on this step is the company's information. (Third party issues are treated separately.)

- ❑ ***General Sufficiency***
  - ❑ What has worked in the past?
  - ❑ What has not worked in the past?
    - ❑ Why has it not worked?
    - ❑ Have employees used work arounds?

- ❑ What work arounds have they used?
- ❑ Why have they used them?
- ❑ Are the work arounds acceptable?
  - ❑ If not, are there ways to address the need that prompted the work around?

- ❑ What is missing?

❑ ***Physical security*** takes two forms: (1) access to the company and (2) access to information.

- ❑ What protocols are in place for entrance to and exit from the premises, buildings, and facilities housing any company trade secrets?
  - ❑ Are there physical barriers to entering and leaving?
  - ❑ Are people required to sign-in/sign-out?
    - ❑ Are employees required?
    - ❑ Are visitors required?
  - ❑ Are badges required?
    - ❑ For employees?
    - ❑ For visitors?
  - ❑ Are logs maintained?
    - ❑ Can all employees view the logs, or just those with a need to know?
    - ❑ Can visitors view the logs?
  - ❑ Are visitors restricted from locations that contain trade secrets?
  - ❑ Are visitors escorted?
- ❑ Does the company maintain video surveillance?
  - ❑ Are backups maintained?
    - ❑ If so, for how long?
- ❑ Is photography or video permitted?
  - ❑ If not, are iPhones, cameras, and similar equipment checked prior to entry into locations in which trade secrets are kept or from which trade secrets can be viewed?
- ❑ Is computer network hardware (including all severs, modems, routers, switches, hubs, and access points) kept in a secure location?
  - ❑ Does access to the location require a key, passcode, or the equivalent?
    - ❑ Is the location kept locked?
  - ❑ Is the hardware itself physically locked down?
- ❑ Are trade secrets physically isolated in a secure location (whether a building, office, room, closet, safe, filing cabinet, or desk drawer)?
  - ❑ Is access to the location restricted to those people who have a need to access the trade secrets?
    - ❑ Is the location sufficiently protected to keep the trade secret out of view?
  - ❑ Does access require a key, passcode, or the equivalent?
    - ❑ Is the location kept locked?
  - ❑ Are trade secrets that are capable of being kept in a folder or container kept in a folder or container?

- ❑ Is the folder or container marked to indicate confidentiality?
- ❑ Are materials containing trade secrets that are outdated or otherwise no longer needed destroyed?
  - ❑ Are documents shredded?
    - ❑ Are they stored in secure waste bins pending shredding?
- ❑ Is the identity of trade secrets appropriately obscured where necessary?
  - ❑ Are codenames or a marking system used for specific confidential information (for example, ingredients)?
    - ❑ Is that carried through on purchase orders, shipping manifests, financial books and records, and other documents?

❑ ***Electronic/technical security*** (like physical security) takes two forms: (1) access to the equipment housing the information and (2) access to the information itself. And, most physical security measures have electronic or technical analogues.

- ❑ Is electronic access to the network secure?
  - ❑ How is the company's network accessed remotely?
    - ❑ Is VPN required?
    - ❑ Is multi-factor authentication required?
    - ❑ Are the protocols sufficient to prevent unapproved connections?
  - ❑ Is the network segmented/partitioned so information can be compartmentalized and access restricted by location on the network?
    - ❑ Are there technological limitations preventing employees from accessing parts of the network where information they do not need to access is stored?
      - ❑ Are there popups or other notices to warn employees when they are accessing portions of the network where trade secrets are stored?
  - ❑ Is information accessible only on a need-to-know basis?
    - ❑ Does all of the information need to be accessible?
    - ❑ Is information segmented to the extent possible so that portions of the secret are kept separate from other aspects of the secret?
    - ❑ Are appropriate identity and access management (IAM) protocols in place?
- ❑ Are all computers and equipment appropriately secure?
  - ❑ Are all laptops and mobile devices physically secured when not in use?
  - ❑ Are all computers password protected?
  - ❑ Are all computers full-disk encrypted?
  - ❑ Are screens set to lock and require reentry of user credentials after a period of inactivity?
    - ❑ Is the period sufficiently short given the location of the computer?
  - ❑ Are all software, hardware, and operating systems up to date?
    - ❑ Are all computers adequately protected with firewall, anti-virus, anti-malware software?
    - ❑ Are all appropriate updates applied, including security updates?
  - ❑ Are employees' administrator functions appropriately limited?
  - ❑ Are there limitations on access to websites?

- ❑ Do all computers and other devices have an appropriate, up-to-date backup system?
  - ❑ Is the use of personal backup systems permitted?
    - ❑ If so, does the company have access to the backups?
    - ❑ Is there a process for removal of company information from personal backups?
- ❑ Can computers and other devices be wiped remotely?
- ❑ Is there an inventory of all computers and other electronic equipment, including their locations?
  - ❑ Does the inventory contain all necessary usernames and passwords?
  - ❑ Is the inventory updated as equipment, passwords, and locations are changed, added, retired, or transferred?

❑ Are all electronically maintained trade secrets adequately protected?

- ❑ Which trade secrets are accessible remotely?
  - ❑ Should they be?
- ❑ Are files containing confidential information maintained in a separate folder?
  - ❑ Does the folder indicate that it is confidential?
  - ❑ Is access to the folder limited to those persons with a need to know?
    - ❑ Is the folder password protected?
    - ❑ Is it encrypted?
- ❑ Do the file names indicate that they are confidential?
  - ❑ Do documents containing confidential information contain legends or other markings to indicate that they are confidential?
- ❑ Are the files containing confidential information password protected?
- ❑ Are the files containing trade secrets encrypted?
- ❑ Are document watermarking, "paper town,"[11] "digital signature," or tracking mechanisms used?

❑ If any of the following is banned, are there technological restrictions on such actions?

- ❑ Copying/downloading trade secrets?
- ❑ Sharing trade secrets?
- ❑ Printing trade secrets?
- ❑ Taking screenshots of trade secrets?
- ❑ Photographing?
- ❑ Emailing?
- ❑ Removing the information from the premises?

❑ Regardless of whether technological impediments are in place, is data loss prevention ("DLP") software used?

- ❑ Are all banned activities monitored?

[11] *See Trade Secrets & Paper Towns*, available at https://www.linkedin.com/pulse/trade-secrets-paper-towns-donal-o-connell/?trackingId=U76HVrnt6jf%2Fwb6RgklLDw%3D%3D.

- ❑ Are alerts set up?
- ❑ If any of the above is not banned, are there popups or other notices to indicate that the information is a trade secret and that require employees to confirm that they intended to engage in the activity?
  - ❑ Are appropriate steps taken to prevent the misdirection or interception of documents containing trade secrets?
    - ❑ Are emails containing trade secrets encrypted end-to-end?
    - ❑ Are digital signatures (authenticating the source of the email and that the content has not been altered) used for emails?
- ❑ Are electronic materials containing trade secrets that are outdated or otherwise no longer needed electronically "shredded"?
- ❑ Are potentially non-secure communication platforms, such as Zoom, Slack, conference call lines, and social media, permitted to be used for work communications?
  - ❑ If so, is confidential information permitted to be discussed or shared?
    - ❑ If so, have all necessary steps been taken to ensure that confidential information is protected?
      - ❑ Have all security settings been set to limit the risk of loss?
        - ❑ For Zoom and other video conference platforms, have each of the following settings been turned on, if available:
          - ❑ Requiring authorized users only?
          - ❑ Requiring a password for entry?
          - ❑ Using the "waiting room" to exclude people until the host permits entry?
          - ❑ Using non-guessable meeting IDs generated for each meeting?
          - ❑ Turning off automatic recording?
          - ❑ Prohibiting recording (unless affirmatively desired and people have been notified)?
          - ❑ Prohibiting screen shots (unless affirmatively authorized)?
      - ❑ Has the information been password protected, encrypted, or otherwise concealed?
      - ❑ Is the audience specifically limited to those who need to know?
        - ❑ Have people been cautioned not to forward invites?
      - ❑ Is the confidential information narrowly tailored to the audience?

- ❑ **Administrative measures**, including in particular **policies and procedures**, are the key to setting and enforcing expectations. Many of the policies will reflect and reinforce the physical and electronic/technological security measures and expectations.
  - ❑ Does the company have all necessary and appropriate policies?
    - ❑ Do the policies convey an appropriate culture of confidentiality?
    - ❑ Do the company's policies reflect all expectations?

- ❑ Are the policies and expectations sufficiently communicated?
- ❑ Do the policies require that employees not bypass physical or electronic security measures?

❑ Are all of the policies consistent with one another?

❑ Does the company require employees to acknowledge that they received, reviewed, and understand and will abide by the policies?

❑ Are employees required to re-acknowledge the policies periodically?

- ❑ How often?
- ❑ Is the requirement followed and documented?

❑ Is there a *trade secret, confidentiality, or information protection policy*?

❑ Does the policy describe the information to be protected?

- ❑ Do the teams who may have a business reason to want to share confidential information (for example, research teams and sales teams) understand what is confidential, what can be shared and when, and what cannot be shared?

❑ Does the policy explain why the information the procedures are in place?

- ❑ Does it explain that the information is critical to the company's success and therefore their and their colleagues' jobs?

❑ Does the policy explain that the protection is extremely important?

- ❑ Does it explain that this is a matter of federal and state civil and criminal obligations?

❑ Does the policy explain that employees have a duty to protect the information?

❑ Does the policy explain how the company expects trade secrets to be protected?

- ❑ Does it provide for multiple levels of confidentiality?
  - ❑ If so, does it explain how to classify information to determine what level of confidentiality applies and what protections are required at each level?
- ❑ Does it recognize that mistakes will happen, such as a failure to appropriately mark confidential documents?
  - ❑ Does it still require that the information be treated as confidential?
- ❑ Does it address applicable physical and electronic/technological requirements, such as encrypting and password protecting documents containing trade secrets?
- ❑ Does it permit trade secrets to be stored off-site in a physical facility or in the cloud?
  - ❑ Does it describe what information can be kept offsite at third-party locations?
  - ❑ Does the policy require encryption of anything stored on the cloud?

- ❑ What level of security is used (*e.g.*, Google offers confidentiality mode[12] for email and Dropbox offers different levels of security depending on the subscription)?
  - ❑ Is the level of security sufficient to protect the company's trade secrets?
- ❑ Is access sufficiently limited?
- ❑ Are the protocols for use of the cloud storage commensurate with those required for network storage?

- ❑ Does the policy limit employee access on a need-to-know basis?
  - ❑ Does it instruct employees not to access information that they do not have a need to know?
  - ❑ Does it require changes in access (whether increasing or decreasing) based on job changes or other changes impacting the need for the information?
- ❑ Does the policy explain that the information may be used only for company purposes, as authorized by the company?
  - ❑ Does it explain with whom and how information can be shared *within* the company?
  - ❑ Does it explain with whom and how information can be shared *outside* the company?
  - ❑ Does it require presentations, speeches, newsletters, press releases, postings on company websites, and other announcements to be pre-screened to ensure that no confidential information is inappropriately shared?
    - ❑ Is there a process for screening potential disclosures?
      - ❑ Is the process sufficiently quick and easy to deter its disregard?
    - ❑ Are internal announcements clear about confidentiality?
- ❑ Does the policy explain that employees may not discuss or view confidential information publicly?
  - ❑ Does it explain not to discuss confidential information where others might overhear?
  - ❑ Do employees know not to display confidential information where others might see it – including on their computer screens?
- ❑ Does the policy prohibit employees from removing trade secrets and other confidential information from the premises, including preventing the information from being taken home?
  - ❑ If not, under what circumstances can such information be taken home?

[12] For a description of confidentiality mode, *see* https://support.google.com/mail/answer/7674059?co=GENIE.Platform%3DDesktop&hl=en.

- ❑ Does it address whether and, if so, how workers are expected to handle any information removed from the premises when they are working remotely?
- ❑ Does the policy explain that confidentiality obligations continue post-employment, including that confidential information cannot be retained, used, or disclosed post-employment?
- ❑ Does the policy explain that employees have a duty to report threats to the company's trade secrets?
- ❑ Does the policy encourage employees to ask for assistance if there is any uncertainty about what is confidential or how to protect it?

❑ Is there a *computer and mobile device use policy*?

- ❑ Does the policy match all physical, electronic, and technical restrictions?
- ❑ Does the policy make it clear that employees are to use computers (including the company's computer network and all computer-related equipment and services) and mobile devices (including smartphones, tablets, and external storage devices) for work purposes only?
  - ❑ Does the policy instruct that employees may not access or use portions of the company's computer network that they are not authorized to access or use?
  - ❑ Does the policy make clear that the devices are not to be used for any unlawful purpose?
- ❑ Does the policy make clear that employees are not to permit anyone else to use their devices, except as expressly required or authorized by the company?
- ❑ Does the policy instruct that employees should not make changes to security and administrative settings or otherwise bypass technological restrictions?
- ❑ Are computers and other devices required to be safely secured when not in use?
- ❑ Do employees have an expectation of privacy when using company equipment?
  - ❑ If not, does the policy sufficiently explain the lack of privacy?
    - ❑ Does it explain that any files, documents, photographs, and other materials stored on the computer may be reviewed by the company?
    - ❑ Does it explain that personal emails, texts, instant messages, and the like that are accessed, sent, received, or stored on company devices are reviewable by the company?
    - ❑ Does it explain that internet activity conducted through the company's computer or internet is reviewable by the company?
- ❑ Does the policy provide for the disposal of computer hard drives and external hard drives?
  - ❑ Are they to be erased?

- ❑ Is there a minimum number of overwrites or other requirements to ensure all data is fully and permanently expunged?
- ❑ Are they to be destroyed?
  - ❑ Is there a process for destroying them to ensure none of the data can be read?

- ❑ Is there a *password* policy?
  - ❑ Does the policy require the use of passwords for all devices (including computers, cellphones, tablets, and external storage devices)?
    - ❑ Does it apply to devices owned by employees, to the extent used for business purposes?
  - ❑ Does the policy establish protocols to reduce the risk that passwords can be guessed or hacked?
    - ❑ Does it provide specific rule-based requirements for password length and strength?
      - ❑ Does it require a minimum length?
      - ❑ Does it require special characters?
      - ❑ Does it require capitalization and lower case?
      - ❑ Does it require numbers?
      - ❑ Does it prohibit dates?
      - ❑ Does it prohibit sequential or repeating letters and numbers?
      - ❑ Does it preclude use of words associated with the company, the person (*e.g.*, their own name or names of family members, birthdays, anniversaries, phone numbers, addresses, pet names, usernames, etc.), or the information?
    - ❑ Does it require passwords to be changed at specific intervals?
      - ❑ Does it preclude the reuse and recycling of passwords?
  - ❑ Does the policy require that passwords be stored in a secure location not accessible or visible to others?
    - ❑ Does it require that stored passwords be encrypted?
    - ❑ Does it permit or require the use of password managers?
  - ❑ Does the policy prohibit sharing passwords?
    - ❑ Does it prohibit employees from asking other employees to borrow their password?
    - ❑ Does it require reporting violations?
- ❑ Is there a *document management and retention policy* covering trade secrets and other confidential information?
  - ❑ Does the policy address where documents containing trade secrets may be stored?
    - ❑ Are trade secrets to all be stored in one place, or is storage decentralized so not all trade secrets are accessible from the same place?
    - ❑ Are documents containing trade secrets permitted to be stored locally, such as on laptops, thumb drives, or physically in

employee offices (as opposed to on networks or the company's designated storage locations)?
- ❑ Does the policy establish a check-in / check-out process?
- ❑ Does the policy permit any of the following?
  - ❑ Copying/downloading trade secrets?
  - ❑ Sharing trade secrets?
  - ❑ Printing trade secrets?
  - ❑ Taking screenshots of trade secrets?
  - ❑ Photographing?
  - ❑ Emailing?
  - ❑ Removing the information from the premises?
- ❑ To the extent any of the above are permitted, under what circumstances are they permitted?
  - ❑ Are there limitations on the quantities of copies?
  - ❑ Are printouts required to be numbered or otherwise controlled?
  - ❑ Are printouts required to be collected from the printer immediately?
- ❑ Does the policy establish appropriate procedures for the disposal and shredding of materials containing trade secrets that are no longer needed?
  - ❑ Are all receptacles for such materials locked?
- ❑ Does the policy address how long documents are retained?

❑ Is there a *clean desk policy*?
- ❑ Does the policy require all confidential materials to be removed from the workspace and secured at the end of the day?
  - ❑ Does it require removal and/or securing when the workspace is not going to be occupied for relatively brief periods?
- ❑ Does the policy require whiteboards containing confidential information to be thoroughly cleaned?

❑ Is there a *social media policy*?
- ❑ Does the policy address who owns social media accounts used for business or mixed purposes?
  - ❑ To the extent that the company owns social media accounts, does the policy require employees to provide all credentials, including usernames and passwords?
    - ❑ Does the policy require employees to follow username and password policies generally and keep the company informed of all changes?
  - ❑ To the extent that employees own all social media accounts, does the policy prohibit commingling of personal and business uses and information on those accounts?
- ❑ Does the policy prohibit the posting, sharing, or discussion of confidential information on or through social media platforms?
  - ❑ Does it explain the risk of communicating confidential information through social media?

- ❑ Does it explain that information can be pieced together from disparate posts and thereby inadvertently reveal confidential information?
- ❑ Does the policy address mandatory privacy settings for accounts used for business?
  - ❑ If the identity of company customers, vendors, or other business partners is confidential, does the policy adequately address restrictions on their disclosure?
    - ❑ Does it permit contacts to be visible to others and, if so, to what extent?
- ❑ To the extent that the policy permits the dual personal and company use of social media accounts, does it provide a process to unwind the commingling?
  - ❑ Does the policy require transfer and deletion of the company's information or transfer of the account upon termination?
- ❑ Does the policy prohibit the employee's use of work-related social media accounts to announce the termination of the employment relationship?
- ❑ Has the policy been updated for changes in applicable laws governing employee personal social media accounts used for work?

❑ Is there a *BYOD (bring your own device) policy*?

- ❑ Does the policy specify which types of devices (including computers and mobile devices) and services are permitted to be used for work purposes?
  - ❑ Does it require company approval before a device or service can be used?
    - ❑ Does it expressly prohibit all devices and cloud platforms that have not been expressly authorized?
  - ❑ Does the policy require compliance with any computer use policies?
  - ❑ Does it specifically address mobile devices such as cellphones and tablets?
  - ❑ Does it specifically address external storage devices (for example, thumb drives, external hard drives, home network backups, home cloud backups)?
    - ❑ If permitted, are they subject to same requirements for other devices (encrypted, storage and disposal protocols, company access, monitoring, wiping, etc.)?
- ❑ Does the policy address privacy and security settings for the device?
  - ❑ Does the policy require personal devices to be password protected in accordance with company password policies?
  - ❑ Does the policy require personal devices to be encrypted?
  - ❑ Are the privacy and security settings up to the same standards as for company-owned devices?
- ❑ Does the policy require all devices to be inventoried with the company?
  - ❑ Does it establish a process for the inventory to be updated?

- ❑ Does the policy provide for sandboxing or segregation of company information from personal information?
- ❑ Does the policy place restrictions on software that may be installed or used?
  - ❑ Does it address security requirements for software that might be permitted?
  - ❑ Is there a protocol for approval of the installation and use of software?
  - ❑ Does it prohibit all software that has not been expressly authorized?
- ❑ Is software used to enforce the policy?
  - ❑ For mobile devices, does the policy address what mobile device management software must be used?
- ❑ Does the policy provide for company technical support?
  - ❑ Does it identify which devices will receive support?
  - ❑ Does it require training before the device can be used?
- ❑ Does the policy delineate where the company's right to monitor and investigate ends and the employee's right to privacy begins?
  - ❑ Does the policy explain that the company has the right to access, monitor usage, and delete information?
  - ❑ Does it permit the company to track and locate the device?
    - ❑ Does it require location services to be turned on?
  - ❑ Does it allow the company to obtain access for litigation, investigations, or other needs?
  - ❑ If the device is backed up on company systems (including in company-controlled cloud-based backup systems), does the policy specify whether, and if so how, the company will handle and protect the employee's information and materials?
- ❑ Does the policy address who else is allowed to use the device?
  - ❑ Are family members permitted to use the device if they have their own password-protected accounts on the device?
- ❑ Does the policy permit other family-owned equipment to be used to access or store company information?
  - ❑ If so, under what circumstances?
- ❑ Does the policy address the removal of company information on the device when the employment relationship ends?
- ❑ Does the policy address what happens if a personal device with company information is lost or stolen?
  - ❑ Does it permit for the entire device to be remotely wiped by the company?
  - ❑ Does it require employees to immediately notify the company if their device is lost or stolen?
- ❑ Does the policy require employees to immediately notify the company if their device has been compromised or if company confidential information is otherwise compromised or at an increased risk?

- ❑ Does the policy provide for discipline for violation?
- ❑ Are there other policies that may address the protection of trade secrets, such as a code of conduct?
  - ❑ Do such policies impact the protection of trade secrets or other confidential information, goodwill, or other legitimate business interests?
  - ❑ Are such policies consistent with the more targeted policies?
- ❑ Does the company require the following *agreements*[13]:
  - ❑ Nondisclosure or confidentiality agreement?
    - ❑ Is it given to everyone who will have access to trade secrets or other confidential information?
      - ❑ All employees?
      - ❑ Contractors?
    - ❑ Is it signed before access to confidential information is given?
    - ❑ Is anyone not required to sign them?
      - ❑ Who?
      - ❑ Why not?
    - ❑ Does it require the return of information and all other property at end of the employment relationship?
      - ❑ If not, is there another agreement that requires the return of confidential information and other company property?
  - ❑ Noncompetition agreement?
  - ❑ Nonsolicitation (of customers) agreement?
  - ❑ Invention assignment?
  - ❑ No raid agreement (also known as a nonsolicitation of employees)?
  - ❑ Does the company require any other restrictive covenants (such as a no-service agreement) from any employees?
- ❑ Are the appropriate agreements required from those employees whose roles create the need for them?
  - ❑ Has each employee signed all necessary agreements?
  - ❑ Has the company signed all applicable agreements?
- ❑ Does each agreement comply with current law, including changes in applicable laws?

Step Three: Evaluate Third Party Implications

The involvement of third parties raises three categories of issues: (1) obligations the company owes to third parties whose information the company is in possession of; (2) obligations of third parties that are in possession of the company's confidential information; and (3) risks associated with bringing in employees (and others) who may possess, use, or disclose information from third parties, such as competitors, former employers, and other trade secret owners.

- ❑ What are the company's obligations to the third parties?

[13] *See Beyond the noncompete*, available at https://www.computerworld.com/article/2524806/beyond-the-noncompete.html.

- ❑ Are they documented in a contract?
- ❑ Are they sufficiently clear?
- ❑ Are the company's protocols sufficient to satisfy the obligations?
  - ❑ Are the company's remote work policies adequate?
- ❑ Which employees are permitted access?
  - ❑ What can they do with that access?
- ❑ What are the consequences of a violation of those obligations?

❑ What obligations are owed to the company by third parties?

- ❑ Are third parties required to sign nondisclosure agreements ("NDAs") before being granted access to the company's information?
- ❑ Are the obligations sufficiently clear?
  - ❑ What are the terms of service for cloud storage facilities?
    - ❑ Do they provide sufficient security?
  - ❑ If the obligation is to protect the company's trade secrets as the third party protects its own, does the company fully understand the third party's protocols?
    - ❑ What are the third party's relevant policies?
      - ❑ What do the policies require?
        - ❑ Are they sufficient?
- ❑ Do the third party's protocols sufficiently address a remote work environment?
- ❑ Which of the third party's employees are permitted to access the company's information?
  - ❑ What can they do with that access?
- ❑ What are the consequences of a violation of the obligations?

❑ Are there protocols in place to ensure that employees do not bring third parties' trade secrets to the company or use or disclose third parties' trade secrets?

- ❑ Does the company make clear to new employees that it does not want trade secrets of others?
- ❑ Does the company explain not to bring, use, or disclose information from prior employers (or others)?
- ❑ Is there a process for reviewing whether an employee (new or existing) has brought, used, or disclosed information?
- ❑ Is there a process for determining whether any third party information been uploaded?
- ❑ How does the company respond to the discovery that information of others has been brought into the company or used or disclosed at or for the company?
- ❑ Does the company evaluate preexisting obligations of potential new employees and restrictions on the employee's conduct?
  - ❑ Does the company evaluate the effect of trade secret obligations on any potential new employee's role for the company?
    - ❑ Does the company take steps to prevent inevitable (inadvertent) use or disclosure of the former employer's trade secrets?
  - ❑ Does the company evaluate any potentially applicable restrictive covenants to which new employees may be subject?

- ❑ Are limitations placed on employees' work to ensure that no other party's confidential information is incorporated into the company's products or services and that employees comply with applicable restrictive covenants?
- ❑ Is there a protocol for when to involve legal counsel (in-house or outside)?

Step Four: Special Considerations in Connection with Work-From-Home (WFH) and Other Remote Work Environments

Work conducted remotely (whether from home or other locations outside of the company's direct control) substantially alters the typical trade secret risk profile in many ways, including the potential for the use of improperly secured Wi-Fi, other people in close proximity, and a lack of formalities that otherwise appertain to typical work environments. Accordingly, a purposeful awareness of and focus on the different and additional risks is necessary, particularly now and as the new normal continues to evolve. And, equally important, employees should be counseled to affirmatively think about their obligations and use basic common sense when company confidential information is at risk.

- ❑ ***Physical security*** in a home workspace should be designed to achieve, as close as possible, the same level of security as in the company's facilities.
  - ❑ Is the workspace a separate, isolated room?
    - ❑ If not, is the space physically separate?
    - ❑ Are other members of the household excluded from the workspace?
    - ❑ Can the workspace be locked when not in use?
      - ❑ If so, is it kept locked when the employee is not using it?
      - ❑ If it cannot be locked, is all equipment and confidential information secure and, to the extent appropriate, stored in locked cabinets or drawers when not in use?
  - ❑ If a clean desk not an option at home, what precautions are in place to protect the company's confidential materials?
    - ❑ Are documents and materials containing confidential information shielded from view from others in the house?
    - ❑ Are documents and materials containing confidential information secured when not in use?
  - ❑ Is printing kept to a minimum?
    - ❑ Are documents removed immediately from the printer?
  - ❑ Is shredding available?
    - ❑ If not, are documents secured until they can eventually be shredded?
- ❑ ***Electronic/technological security*** requirements are heighted in the home where home networks tend to be less secure than those at an office.
  - ❑ Is the home network secure?
    - ❑ Is the network ID (SSID) broadcasted?
    - ❑ Is Wi-Fi password protected?
      - ❑ Is the password sufficiently secure?
    - ❑ Does the router meet current security standards?
      - ❑ Is the firmware updated?

- ❑ Is an appropriate firewall in place?
- ❑ Are computer screens set to lock when not in use?
- ❑ Have any members of the household used any device that is being used for work?
  - ❑ Are the devices checked for malware?
  - ❑ Are appropriate safeguards in place to avoid compromising company information?
- ❑ Are smart devices like Alexa, Siri, and Google Assistant (as well as other video and/or listening devices such as baby monitors) turned off or sufficiently distant (or directed away) from the workspace to avoid them picking up sound or video?

❑ ***Administrative measures*** for a work-from-home environment should explain that the same rules that apply at the office apply as close as possible to the home workspace. Given the prevalence of potentially non-secure communication platforms like Zoom and Slack, specific reminders about the requirements concerning their use should be provided.

- ❑ Do employees understand that all of the same rules apply when it comes to protecting the company's trade secrets and other confidential information?
  - ❑ Is it clear that the informality of home does not translate to a relaxation of the need to protect and protocols for protecting trade secrets and other confidential information?
    - ❑ Have employees been told that it is critical to follow the same policies and procedures for marking and handling documents and information?
      - ❑ Have employees been told that if information was not to be accessed, printed, used, shared, or disclosed before, it should not be accessed, printed, used, shared, or disclosed now?
- ❑ Have employees been instructed that confidential information should not be viewed where others may see it?
  - ❑ Is it clear that this includes on their computers in their home?
  - ❑ Are all video cameras turned off or sufficiently directed away from the workspace?
- ❑ Have employees been told that confidential information should not be discussed publicly or anywhere else others may overhear it?
  - ❑ Are phone calls or video calls made from or received in a location – whether inside the house, in the yard, or elsewhere – where no one can hear?
    - ❑ When calls are on speaker, is the volume sufficiently low to avoid anyone from hearing?
      - ❑ Can headphones be used (to address the inbound portion of the communication)?

Step Five: Communicate and Reinforce Expectations

Having policies and procedures that no one understands, remembers, or follows undermines the reason for having them in the first place. The key to ensuring their ongoing utility is employee

education and training on a periodic basis. This is particularly true with remote and hybrid-remote workers, which may require very different processes and procedures from what they are used to.[14]

- ❑ Is trade secret training provided at the start of employment in connection with employee onboarding and orientation and then at periodic intervals during the course of employment?
  - ❑ Do the trainings explain what trade secrets are, why they are important to the company, and that protection of the company's trade secrets is of critical importance?
  - ❑ Do the trainings instruct employees to review and comply with the company's policies and procedures?
  - ❑ Do the trainings instruct employees to comply with any preexisting obligations to prior employers?[15]
    - ❑ Do they explain that the company does not want trade secrets of others?
    - ❑ Do they instruct employees not to bring, use, or disclose information from prior employers (or others)?
  - ❑ Do the trainings cover important restrictions on access to and use of trade secrets?
    - ❑ Do they reinforce that employees should not access (or try to access) information that they do not have a right to access?
    - ❑ Do they reinforce that employees should not access (or try to access) parts of the network they do not have a right to access?
    - ❑ Do they reinforce that employees should not use company information for any purposes other than for the company's benefit, as authorized by the company?
    - ❑ Do they instruct employees to review their contractual obligations?
    - ❑ Do they reinforce obligations to third parties?
  - ❑ Do the trainings address how to avoid inadvertently installing malware?
    - ❑ To the extent the use of USB devices is permitted, are employees instructed that such devices – including thumb drives distributed at conferences – may contain malware?
    - ❑ Are employees trained on the following:
      - ❑ To be suspect of emails from people they do not know?
      - ❑ That unusual language, broken English, typographical errors, and other mistakes in emails, texts, and similar communications is oftentimes an indication that the message is a scam?
      - ❑ Not to click on links or open files that they were not expecting until their authenticity is confirmed?

[14] Trainings can be accomplished in many ways, oftentimes complimentary of one another. For example, video instruction may be an effective way to sensitize employees to critical issues. *See*, *e.g.*, *Protecting Trade Secrets While Working Remotely*, available at https://www.youtube.com/watch?v=ZqA7Dk0pl78.

[15] Recipients of job offers can (and generally should) be reminded of their obligations to their former employers. This can take many forms, including "empty briefcase" letters and training videos. *See The Exit Plan: Being a Good Leaver*, available at https://www.youtube.com/watch?v=TLV1q0x0OM0.

- ❑ To investigate any request for information when the request was not anticipated or seems unusual?
- ❑ To check the return address in emails before responding to the email?

❑ Do the trainings encourage employees to ask for assistance if there is any uncertainty about what is confidential or how to protect it?

❑ Does the company ask employees to watch for and report suspected actual or potential misappropriation or other policy violations?

❑ Does the company explain that employees should report not just intentional misconduct, but inadvertent disclosures and other risks of improper use or disclosure of confidential information belonging to the company or third parties?

Step Six: Monitor Compliance

Trust but verify. While companies may hope and assume that their employees will comply with all security measures, policies, and trainings, there is no foolproof way to ensure it. Accordingly, companies should consider monitoring for compliance – whether on a continuous or spot-checking basis. Even when monitoring is limited and unlikely to catch misconduct or inadvertent trade secret exposure, it may still have the benefit of encouraging employees to think twice.

❑ Does the company monitor network activity and email traffic?

❑ Are alerts sent for suspicious or prohibited activities, including, for example, the following:

- ❑ Spikes in usage or data transfer?
- ❑ Large downloads from or uploads to the network?
- ❑ When employees connect to unauthorized file sharing and FTP sites?
- ❑ Substantial printing?
- ❑ Access to certain areas of the network?
- ❑ When USB storage devices are connected, particularly if they are prohibited?

❑ Are emails screened for attachments potentially containing trade secrets or keywords disclosing trade secrets?

- ❑ Are flagged emails rerouted to appropriate for review?

❑ Does the company check that all policies and procedures being followed?

❑ Have all employees signed the necessary acknowledgements and agreements?

❑ Have all employees undergone the required trainings?

❑ Is there a process for reviewing whether employees have brought or used third-party information?

- ❑ Is there a process to address confidential information discovered to have been uploaded, used, or incorporated into company products or services?

❑ Is there appropriate discipline if policies or procedures have not been followed?

Step Seven: Exit Practices and Procedures

Even in the best of circumstances, departing employees pose a significant risk to a company's information and customer relationships. These risks are significantly increased in times of crisis and economic turmoil, particularly when employees are furloughed, laid off, feeling disconnected, or just in need of a change. Accordingly, it is extremely important to take this opportunity to lock down as much as possible at this last stage of the employment relationship. This involves four basic steps: (1) conducting the exit interview; (2) terminating post-employment access; (3) recovering all equipment; and (4) evaluating the potential risks.

- ❑ ***Exit interviews*** are ideally performed in person, though when that is not possible, they are best conducted through videoconferencing tools like Zoom. The purpose of the exit interview (from a trade secret protection standpoint) is to understand what, if any, risks are posed by the employee's future plans and to remind the employee of ongoing obligations to the company.
  - ❑ Where is the employee going?
    - ❑ What is their new role?
    - ❑ What are their duties?
    - ❑ Will the new job violate their ongoing obligations?
    - ❑ Will it place the company's trade secrets (or goodwill or other legitimate business interests) at risk?
      - ❑ Is there a way to protect the company's interests while allowing the employee to work in the anticipated role?
  - ❑ Does the company remind employees about their ongoing confidentiality obligations and any other obligations?
    - ❑ Is the employee advised not to retain, use, or disclose company information?
    - ❑ Is the employee provided a copy of all of relevant agreements they have with the company (nondisclosure agreements, noncompetition agreements, nonsolicitation agreements, and any others)?
    - ❑ Is the employee asked to acknowledge the agreements?
  - ❑ Is the exit interview documented?
    - ❑ Is there a form with questions to ask?
      - ❑ Is it completed each time?
- ❑ ***Post-employment access*** to any company equipment and information must be terminated immediately, absent some continuing relationship necessitating and warranting continued access. This is also true in connection with furloughed employees, who, although not officially separated from the company, are not working and therefore should no longer have access to company equipment or information.
  - ❑ Does the company immediately terminate the employee's access to all company resources and accounts, including each of the following:
    - ❑ Computer network?
    - ❑ Email?
      - ❑ Are the employee's emails forwarded (to the appropriate person)?
    - ❑ Phone system and voicemail?

- ❑ Are the employee's phone calls and voicemail messages directed to the appropriate person?
- ❑ Company cloud storage accounts?
- ❑ Third party platforms used for business, including, for example, DropBox, Microsoft 365, Commvault, and contact management services like Salesforce?

❑ To the extent not covered by the above, does the company change all of the employee's passwords upon termination?

❑ Is there a process for remote wiping or purging company information from the employees' personal devices?

❑ Is there a process to disable any physical access cards retained by the employee?

❑ ***Recovery of company-owned equipment, materials, information and other property*** is a critical step in the departure process.

❑ Is there a process to collect all electronic equipment, such as laptops, tablets, smartphones, external storage devices, and other devices?

- ❑ Is the company set up to arrange (and pay) for the equipment to be shipped back when workers are not coming into the office?
  - ❑ If that is not feasible, is the timing such that a forensics company needs to remotely gather a forensic image of a device's hard drive?
- ❑ Are all devices returned intact?
  - ❑ Have they been wiped or factory reset?
    - ❑ Was it authorized?
  - ❑ Do iPhones and other smartphones include any SIM cards?
    - ❑ Does the company have the password?

❑ Will the employee cooperate with the company to disentangle personal information and files (*e.g.*, family photos) from work devices and work information?

- ❑ Are any personal photos in fact what they purport to be and not photographs of company information?
- ❑ Does the employee understand what information the company owns, including, for example, customer contact information, projects on which the employee worked, PowerPoint presentations the employee prepared for work?

❑ Is there a process to collect all hardcopy documents and materials?

❑ Is there a process to collect all other property, including access keys, badges, credit cards, etc.?

❑ Is all returned property inventoried?

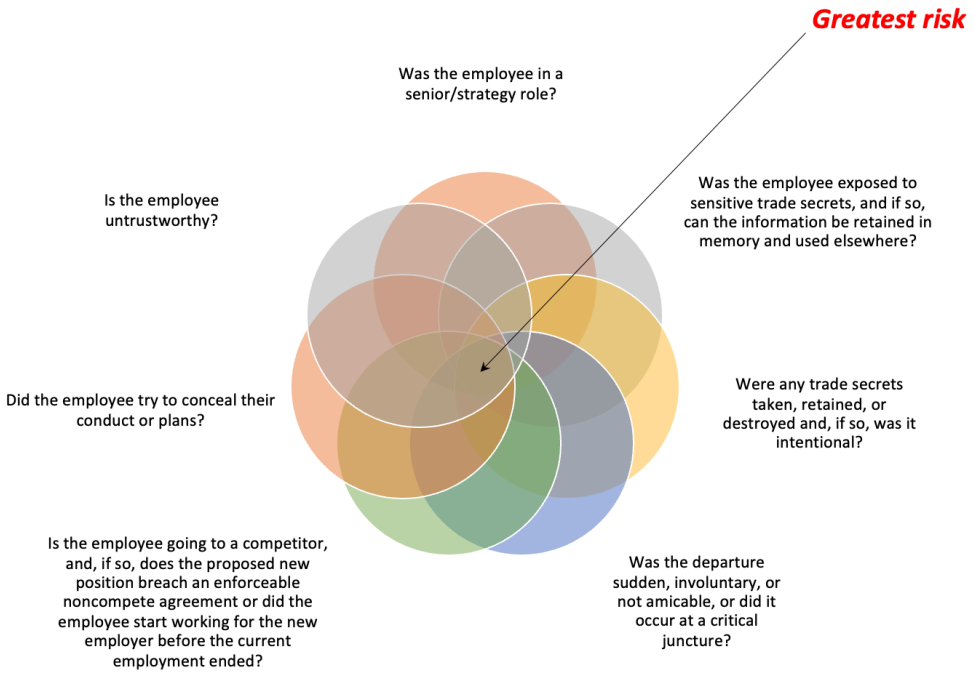
❑ Will the employee certify that everything has been returned and nothing has been retained?

❑ Have remaining employees been advised of any restrictions regarding communications to or from the furloughed or former employee?

❑ ***Evaluation of the risk*** to the company's information will often require nothing more than a quick determination that the employee poses no substantial threat. Other times, it may be readily apparent that the employee poses a significant threat. In many cases, however, the process is more involved. When the answer is not obvious, the company can ask a

series of questions to assess the level of threat and appropriate next steps, up to and including full enforcement of the company's rights. When all of the questions are answered in the affirmative, the risk will typically be at its height.

- ❑ How great a risk does the employee pose based on the following seven, high-level questions? (See Venn diagram below for a visual assessment.)
  - ❑ Was the employee in a senior / strategy role or exposed to sensitive trade secrets?
  - ❑ Can the information to which the employee was exposed be retained in memory and used elsewhere?
  - ❑ Was the departure sudden or did it occur at a critical juncture?
  - ❑ Is the employee going to a competitor?
  - ❑ Will the new role result in the inevitable use or disclosure of the company's information?
  - ❑ Was the departure involuntary (or otherwise not amicable)?
  - ❑ Did the employee take, retain, or delete information and, if so, was it intentional (as opposed to part of the normal course or work or routine backups)?



- ❑ Does the risk warrant a forensic review of the employee's computer?
  - ❑ Does the email history reveal any misconduct?
    - ❑ Does it suggest that information was sent to someone unauthorized to receive it?
      - ❑ Does it show information being sent to the employee's personal email address or to someone else closely associated with the employee?
      - ❑ If so, is there a history of such conduct, or did it not happen until at or near the end of employment?

- ❑ Does it reveal any inappropriate customer communications?
- ❑ Does it reveal anything about the timing of when the employee began job searching or anything that might contradict anything that the employee told the company?

- ❑ Are there any logs that reveal that the employee accessed, downloaded, or printed information or documents at a time, in a volume, or of a nature that should not have been accessed, downloaded, or printed?
- ❑ Were USB storage devices connected?
  - ❑ Did the employee routinely use USB storage devices?
  - ❑ Were any of the devices not returned?
  - ❑ Does the timing of the connection reveal any improper conduct?
    - ❑ Was it at odd hours (*e.g.*, late at night, early in the morning, or otherwise when the employee's conduct would likely not be noticed)?
    - ❑ How does the timing of the connections relate to the timing of the employee's access to the company's computer files?
- ❑ Did the employee use Dropbox, iCloud, Google Drive, Microsoft 365, Commvault, or other online storage or backup sites?
  - ❑ If so, is a review of those accounts warranted and possible?
- ❑ Does the internet search history reveal any improper conduct?
  - ❑ Does the search history reveal anything about the timing of when the employee began job searching or anything that might contradict anything that the employee told the company?
  - ❑ Does the search history suggest that the employee investigated how to wipe devices or otherwise delete evidence of wrongdoing?

- ❑ Is there a process to monitor for and assess signs of misconduct?
  - ❑ Is the employee's work email forwarded to someone at the company to watch for misdirected emails from customers?
  - ❑ Are the employee's social media accounts monitored for evidence of improper conduct?
    - ❑ Has LinkedIn been updated?
  - ❑ Are there unexpected changes in the marketplace?
    - ❑ Is the company losing business that it expected to get?
      - ❑ If so, is it likely due to the employee's conduct or something else, like changing market conditions?
    - ❑ Is there a sudden new competitor?
      - ❑ If so, is the employee involved?
  - ❑ Has the employee attempted to access the company's systems?
    - ❑ Under what circumstances?
      - ❑ Did the company fail to turn off access?
  - ❑ Is there a form (digital or electronic) for reporting and investigating an incident?
- ❑ Is a private investigator warranted?

Step Eight: When All Else Fails, Have a Plan and Implement It

While the goal is to avoid the need for enforcement of the company's rights (in particular through lawsuits), unfortunately no amount of protection efforts, education, or training will prevent some people from doing something they should not. Accordingly, the company needs to have an "incident response plan" ("IRP") – and a designated person (or team) responsible to lead the incident response – before there is an accidental or intentional disclosure or use of the company's confidential information.

- ❑ Is there a person or team responsible for responding to misappropriation or breaches of restrictive covenants?
  - ❑ Who is the primary point of contact (who will be notified immediately when there is a potential problem)?
  - ❑ Does legal counsel need to be involved?
    - ❑ In-house, outside, or both?
- ❑ Is there a reason not to send a letter reminding the departed employee of their confidentiality obligations and any other post-employment restrictions?
- ❑ Is a cease and desist letter warranted?
- ❑ Should the new employer be contacted?
  - ❑ If so, by letter or telephone?
  - ❑ Is there a preexisting relationship with the new employer than can be used to attempt to amicably resolve the matter?
- ❑ Is litigation necessary?
  - ❑ If so, is a temporary restraining order, preliminary injunction, or similar emergency relief necessary?
    - ❑ Does the need for injunctive relief take into account the current circumstances?
      - ❑ Are damages a sufficient, even if not complete or satisfactory, remedy under the circumstances?
    - ❑ If restrictive covenants are involved, can they be enforced?
      - ❑ Was the employee furloughed or laid off?
        - ❑ If so, does it affect enforcement?
      - ❑ Are the courts enforcing restrictive covenants in the jurisdiction?
    - ❑ Are the courts available for injunctive relief in sufficient time?
      - ❑ If not, are courts in other potentially appropriate venues available given the current circumstances?

Takeaways

Courts help those who help themselves. But companies are best off protecting themselves so they don't need the courts. Accordingly, following this checklist – not prescriptively, but as a guide to think through the issues – should help companies quickly identify what they're doing right and what they need to do differently.