HRtelligence

WEBINAR OVERVIEW

Guidance on Protecting Proprietary Information And Marketing While Maintaining Employee Privacy

August 23, 2023

Intro/Setting the Stage

- The Importance of Protecting Your Company's Data and Intellectual Property

What Constitutes Confidential Information?

- Examples of Confidential Information
- What is a Trade Secret?
    - Statutory Definitions under the UTSA
    - Statutory Definitions under the DTSA

Strategies for Maintaining Confidentiality in The Workplace

- Confidentiality Agreements
- Develop Confidentiality Training and Policies
- Create an Employee Exit Procedure
- Dealing with Breaches in Confidentiality

Protecting Confidential Information While Employees Work Remotely

What Is Cybersecurity?

- Benefits of Establishing a Workplace Cybersecurity Program
- Variations of Cybersecurity Measures Among Different Types of Employers

HRtelligence TIPS

WEBINAR OUTLINE

I. INTRO/SETTING THE STAGE

The Importance of Protecting Your Company's Data and Intellectual Property

- Like most all modern companies, your company and its staff face tremendous market pressure to protect the trade secrets and confidential information belonging to the Company, its customers and its collaborators.
- Successful protection of confidential information allows the Company to keep staff employed, grow staff opportunities, serve existing customers, and attract new customers.
- The Company's confidential information falls into two main categories: a) information developed and owned by Company; and b) information temporarily given to Company by its customers, collaborators and others.

Notes: Protecting your company's data and intellectual property is important as it keeps your information from being stolen from outside parties and helps you maintain your competitive edge in the market. By implementing company policies and strategies that properly secure your proprietary information, you can prevent employees from leaking critical company data and ideas to competitors.

II. What Constitutes Confidential Information?

Confidential information covers many types of information. Generally, confidential information includes any secret information that gives the Company a competitive advantage.

If a staff member is unable to determine whether information is confidential, the staff member should assume the item is confidential until otherwise confirmed by Company management. Examples of confidential information might include:

- Company information marked "Confidential"
- Company customer targets and proposals
- Software application designs and specifications
- Details contained in signed contracts
- The dimensions, staff numbers and resources located in an office location
- Project status updates and reports
- Business plans
- Company databases
- Company pricing programs
- Company strategic plans
- Company financial records
- Employee files, compensation and benefits

- Company research and development projects
- Company marketing strategies and programs
- Company's new customer targets
- Company's new business development initiatives
- Company reports and analysis
- Contract and negotiation strategies
- Company processes, techniques and systems used or considered for use
- Hardware, software, and database passwords
- Software code created for a Customer
- Customer information (and any third party items) marked as "Confidential"
- Customer systems and databases
- Customer business, financial and sales data.

What Is a Trade Secret?

Employers must identify what types of trade secrets warrant protection before they can implement protective measures.

Protective measures may differ based on the nature and value of the trade secret being protected. Employers may protect electronically stored trade secrets using the cybersecurity measures described below.

There are many types of trade secrets that employers may seek to protect:

- Customer or potential customer lists
- Employee lists
- Employee agreements or other information regarding wages or benefits
- Cost, price, billing, and profit information and methodology
- Marketing and business plans
- Customer service and supply preferences or requirements
- Designs, formulas, recipes, and computer code
- Contracts and contract negotiations –and–
- Databases and spreadsheets containing logistical data and statistics

Statutory Definitions of Trade Secret

Employers alleging trade secret misappropriation must first prove the misappropriated property was a "trade secret" as defined under most state Uniform Trade Secret Acts (UTSA) (or other local trade secret statutes) or the Defend Trade Secrets Act of 2016 (DTSA), 18 U.S.C. § 1836. See Trade Secret Fundamentals. For additional detail on the DTSA, including, among other things, an analysis of available DTSA remedies, see Defend Trade Secrets Act (DTSA) and Other Legal Claims and Recourse to Protect Employers' Confidential Information and Trade Secrets.

UTSA § 1.4 defines trade secret as:

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.
Unif. Trade Secrets Act § 1(4).

The DTSA provides a similar definition of trade secret:
The term "trade secret" means 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 value from the disclosure or use of the information.
18 U.S.C. § 1839(3).

Notes: The measures an employer takes to protect confidential information and data may determine the extent of legal protection afforded to their trade secrets. Both the UTSA and DTSA require employers to make ''reasonable efforts'' or take ''reasonable measures'' to keep information confidential for such information to qualify as a trade secret. What constitutes a reasonable measure may depend on the type of trade secret being protected. As described below, reasonable efforts usually consist of a combination of security measures.

Note, however, that the DTSA provides a carve-out that immunizes from liability under both federal and state trade secret law an individual's disclosure of a trade secret:

- *To the government or to an attorney for the purpose of reporting or investigating a suspected violation of law –or–*
- *Made under seal in a court filing*

18 U.S.C. § 1833(b).
*The DTSA requires employers to either provide notice of this immunity in their confidentiality agreements or cross-reference a policy document that explains its reporting policy for suspected violations of law. Id. A small number of federal courts, interpreting the DTSA immunity provision, have treated it as an affirmative defense and required the party asserting it to support it with factual evidence. See Unum Grp. v. Loftus, 2016 U.S. Dist. LEXIS 168713 (D. Mass. Dec. 6, 2016); 1-800 Remodel, Inc. v. Bodor, 2018 U.S. Dist. LEXIS 225000, at *16–*17 (C.D. Cal. Oct. 17, 2018).*

Strategies for Maintaining Confidentiality in the Workplace

Employees often pose the biggest risk to company confidentiality. When employees have access to private information or documents, they could intentionally or unintentionally share ideas and other private information. Thankfully, there are ways to mitigate this risk.

Confidentiality Agreements

- Confidentiality agreements, also known as non-disclosure agreements, set forth what types of information the employer considers confidential, the employer's policy against improper use or disclosure of such information, and the consequences of violating the employer's confidentiality policy.
- Employers may provide the confidentiality policy in a non-disclosure agreement, an employee handbook, or a stand-alone policy issued with new-hire or onboarding paperwork, or conspicuously post the confidentiality policy in the workplace (or make it available through a combination of some or all of the above methods). It is recommended that, while the employer has options as to how to distribute these agreements, it is best practice to receive a signature acknowledgment.

Develop Confidentiality Training and Policies

- **Confidentiality training should be a key component in every company's onboarding process**. Companies should discuss confidentiality with employees and consider adding it to employee handbooks and online training.
- **Teaching employees how to handle and dispose of sensitive material is an excellent place to start**. In addition, companies should provide employees with information about confidentiality laws and the legal repercussions of violating company privacy policies.
- Having confidentiality policies for employees can also be helpful.

Notes: For example, establishing a "clean desk policy" is a great idea for office-based companies. ***A clean desk policy requires employees to clear confidential documents from their desks and workspaces*** *at the end of each day. It could also mean locking up documents, laptops, computer screens, and USBs when they're not getting used. By simply storing confidential documents properly, companies can better protect sensitive information.*

Create an Employee Exit Procedure

- **Businesses should create a standardized offboarding process for departing employees**. This type of process should involve an exit interview, but should also outline how employees return company property and forfeit their access to confidential information.
- To ensure confidentiality, **the exit process should also involve disabling a departing employee's company access**. This may include disabling their email account, login information, and remote access. Doing so will protect business records and other important data.
- After an employee leaves, some companies may also choose to change company-wide passwords that access sensitive company information and important software. This practice can be especially crucial if a departing employee is terminated.

Notes: Failing to disable departing employees' accounts and change passwords can lead to security breaches that negatively affect a business. Therefore, these precautions should be taken immediately.

Having a process better ensures that employees don't take confidential material with them, reducing the company's exposure to security risks.

Dealing with Breaches of Confidentiality

- Even when a business takes steps to maintain and ensure confidentiality, **breaches can still take place**. Therefore, it can be a **good idea to create a response plan**.
- A response plan should address how to assess the damage or risk of a confidentiality breach and include steps to secure the information or remedy the situation. Steps may include removing information from the source, locating copies of sensitive material, and taking legal action.

Notes: Companies can plan for specific situations, such as published trade secrets or an employee divulging information to competitors. If the latter occurs, the employer would terminate the employee or remedy the situation as specified in the Employment Contract.

In a response plan, ***the more circumstances a company takes into account, the more prepared it will be should confidentiality violations occur****.*

Protecting Confidential Information While Employees Work Remotely

Consider taking the following steps to protect trade secrets in the hands of employees working at home:

- **Repeatedly remind workers it is their responsibility to ensure that confidential information remains confidential while in their home worksites**. They must stay aware of and alert to potential vulnerabilities.
- **Reiterate to employees that they may not transmit or maintain the employer's confidential information except as authorized by the employer**. This requirement applies to personal email accounts, cloud accounts, social media, and other electronic communications and platforms.
- **Prohibit workers from printing documents as much as reasonably practical while they work from home**. To the extent that employees need hard-copy confidential materials, tell the WFH employees not to discard them in their ordinary trash. Require them to retain all confidential documents in secure (locked) locations at their homes so they may be securely disposed of once the employer's workforce returns to the office.
- **If reasonably possible, direct the workforce to connect to the employer's business's network as securely as possible, such as through a VPN**. Consider requiring two-factor authentication for access to the employer's business's VPN or remote network.
- **Remind WFH workers to password-protect their home WiFi system**. They should work with the employer's IT personnel so that communications including confidential information are encrypted.
- **Educate workers about malicious emails, SMS messages, and other communications designed to infiltrate the employer's business's network**.
- **If possible, implement a system that notifies the employer's IT department whenever an employee downloads, copies, prints, or deletes a significant**

amount of data from the employer's business network. The activity may turn out to be legitimate, but the employer should investigate it.
- **Give employees a specific "go to" person should they have any questions or concerns about working at home with company confidential information**.

Notes: Also, remember the protection of an employer's confidential information goes beyond the regulation of the employer's immediate workforce. Employers should consider asking vendors, suppliers, and outside professionals with access to the employer's confidential information what they are doing to protect the employer's trade secrets and implement guidelines they must follow.

What is Cybersecurity?

- In the digital age, employers store most information on computer systems and networks. Cybersecurity refers to the technological protection of computers, networks, programs, and systems from attack, damage, and unauthorized access.
- Cybersecurity is particularly important for employers because they maintain a wide variety of confidential information on computer systems and networks that they must protect not only from data breaches that anonymous hackers cause, but also from trade secret misappropriation that their own employees commit.
- Employers must protect their trade secrets because, among other reasons, trade secrets provide employers with commercial advantages over their competitors.

Benefits of Establishing a Workplace Cybersecurity Program

- Establishing and maintaining formalized workplace cybersecurity programs can help minimize the risk of trade secret misappropriation by reducing opportunities for unauthorized parties to gain access to an employer's networks, computers, and data.
- Employers with a well-established cybersecurity program are also better positioned to respond and recover faster in the event of a data breach or trade secret misappropriation.
  Notes: Recovery speed is significant because it shows the employer has an important and protectable interest, which it must demonstrate to a court to establish a trade secret misappropriation claim. Additionally, faster recovery allows an employer to mitigate and limit the damage that may result from a data breach.

Variations of Cybersecurity Measures among Different Types of Employers

- Cybersecurity measures are unlikely to vary significantly based on the type of information that an employer seeks to protect.

  Notes: While a manufacturing company will have different types of trade secrets from a retail company (e.g., blueprints of machines versus customer lists), the electronic storage of trade secrets via a computer, software system, or other online repository means it is possible that they can each be protected by the same or similar cybersecurity methods
  .
- However, the size of the employer may determine what kinds of cybersecurity measures are appropriate. Certain small companies may have fewer resources and personnel than large companies.

*Notes: This means cybersecurity oversight may rest with one or a few individuals rather than an information security team, for example. Small companies may also not have the financial resources to invest in information technology or to install many types of software and programs to protect their computers and network. That does not mean that a court will find that smaller companies fail to take reasonable steps to protect their trade secrets. For example, at least one court held that keeping customer files in a closed file drawer, informing employees that files were confidential, and limiting employee access to the customer files were ''reasonable for a small tailor shop to maintain the secrecy of a customer list and customer information.'' Elmer Miller, Inc. v. Landis, 253 Ill. App. 3d 129, 134 (Ill. App. Ct. 1993); see also Aurora Internal Med., Ltd. v. Moore, 2011 Ill. App. Unpub. LEXIS 2614, at *48 (Ill. App. Ct. 2011) (an employer's efforts must be ''reasonable under the circumstances'' with one of the circumstances being the ''size of the business'').*

- Regardless of size and resources, employers should use as many of the cybersecurity measures described below as possible in the event they must demonstrate to a court that they took reasonable steps to protect their trade secrets.