Webinar 10 – May 28, 2025

Strategies on Securing and Protecting Proprietary Information

WEBINAR OUTLINE

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

WHAT IS CYBERSECURITY?

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

HRtelligence TIPS

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.

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 it 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).

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.

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.

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.

Identify what information you are trying to protect:

Employers can have a hard time knowing what they should consider secret. It's hard to control employees' access to information and equipment unless you know what you're trying to protect.

In deciding what's confidential about your business, look at:

- the extent to which the information is known outside the business
- the extent to which the information is known by employees and others involved in the business
- the value of the information to the business and its competitors
- the amount of effort or money expended by the business in developing the information
- the ease or difficulty with which the information could be properly acquired or duplicated by others

Specific items to protect. Some specific items that can be protected by a confidentiality clause or agreement include:

- trade secrets
- inventions
- discoveries
- data
- formulas
- business methods
- processes
- machines
- manufacturers
- compositions

Customer and client information. Another type of information that you may want to protect is sensitive customer or client information. In certain industries and professions, your employees may become privy to information that you and your customers or clients would not want to be made public. If this is true for your business, you may want to consider a confidentiality policy to protect it.

Once you have an idea of what you want to protect, if anything, you can better devise a strategy for how to protect confidential information.

Protecting confidential information

The type of information that you're trying to keep secret, and how many employees have access to it, will play a role in deciding how you choose to handle confidentiality issues.

There are some basic steps you can take to protect your business's information. Some of these steps may seem too drastic for your purposes. Use only those that you feel are necessary and that will achieve a degree of security with which you are comfortable. These are also good steps to take in developing your confidentiality policy:

- Explain to employees the need to protect certain types of information.
- Define as much as possible the type of information that you are trying to protect.
- Prohibit the dissemination of confidential information.
- Educate employees on the kind of situations in which they might unwittingly reveal confidential information.
- Explain the penalties for violating the company's policy.
- Make employees sign a noncompete agreement when they are hired.
- Remind employees that work product belongs to the business, not to individual employees.
- Set up procedures for identifying and safeguarding company proprietary information (for example, establish passwords for computers).
- Be prepared to prosecute the theft of secrets.

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.

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.

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.

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.

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.

- 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.

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

Employers have a crucial role in the necessary tools and resources to protect their organization's assets. Here are some key responsibilities for employers:

Identify what information the company would like to protect and create an effective confidentiality and security policies.
Establish clear and comprehensive security policies and procedures that outline acceptable use of technology, password requirements, data handling and encryption, and incident response protocols. Regularly communicate and enforce these policies to ensure employee compliance. Conduct periodic reviews and updates to align with evolving cyber threats and changing regulatory requirements.

Employee Training and Awareness
Employers should invest in regular training and awareness programs for employees. Educate employees on the latest cyber threats, such as phishing, ransomware, and social engineering attacks. Reinforce good security practices, password hygiene, safe web browsing, and incident reporting protocols. Create a culture of cybersecurity awareness where employees feel comfortable seeking guidance and reporting potential security incidents.

Access Controls and User Privileges
Implement proper access controls and user privileges to limit unauthorized access to sensitive data and systems. Employ the principle of least privilege, granting employees access only to the resources required to perform their job functions. Regularly review and revoke access privileges for employees who change roles or leave the organization to prevent lingering access vulnerabilities.

Regular Software Updates and Patch Management
Maintain an effective software update and patch management process. Regularly update operating systems, applications, and firmware to ensure the latest security patches are

applied promptly. Consider implementing an automated patch management system to streamline this process and reduce the risk of unpatched vulnerabilities.

With robust security measures, ongoing training, and a proactive approach to cybersecurity, organizations can significantly reduce the risk of cyber incidents, protect sensitive information, and safeguard their reputation.