“Early Bird” Session

CREATING A CULTURE OF CONFIDENTIALITY FROM ONBOARDING TO OFFBOARDING

Adam T. Dougherty (Moderator) – Ogletree Deakins (Dallas)

Heidi Kuns Durr – Ogletree Deakins (St. Louis)

David P. Thatcher – Ogletree Deakins (Atlanta)
Companies know their confidential information needs to be protected and they expect their employees to handle such information with care. Employees obviously are not to share it with others or steal it for themselves. Yet, companies continue to have problems with the loss or misuse of their confidential information. Companies can combat this problem by intentionally and thoughtfully creating a culture of confidentiality in the workplace: to help their employees recognize that they have a duty to maintain the confidentiality of the company’s data even when they may think it interferes with job efficiency or to strengthen the company’s position in the event that litigation arises.

There have been several recent news articles of employees accused of stealing their employers’ confidential information. In February 2019, a 30-year employee of a cast-iron manufacturer was found guilty of seven counts of theft of trade secrets after he took his employer’s data and documents before quitting to work for a rival company. In the summer of 2018, two cancer researchers at GlaxoSmithKline pleaded guilty to conspiring to steal the company’s biopharmaceutical trade secrets. One researcher claimed she did not understand the material she emailed to her private account and then onto others—including portions of her own patent application—was considered trade secrets. The second researcher admitted he set up a company to market and sell the cancer drug research in China.

In July 2018, a General Electric engineer was charged with stealing the company’s trade secrets involving its turbine technologies and hid data files in a digital photograph of a sunset. The employee allegedly then emailed the picture to his personal email account. That same month, a former Apple employee was captured at the airport after he allegedly stole the company’s secret plans for self-driving cars. The company’s suspicions were raised after the employee announced his resignation and plans to work for a Chinese autonomous and electric vehicle startup immediately after returning from a trip to China while on paternity leave. The employee had downloaded confidential technical documents and placed them on his wife’s laptop. Surveillance footage and badge swipe records found that the employee had entered Apple’s autonomous vehicle labs and left with a keyboard, some cables, and a large box, all while he was on paternity leave.

It is no surprise that these types of thefts are costly to companies. According to the Association of Certified Fraud Examiners (AFCE), asset misappropriation schemes (including misuse of assets) are the most common types of fraud, resulting in a median loss of $114,000 to an organization.

But theft is not the only way companies lose their confidential information. In fact, a 2017 survey conducted by Dell-End User Security found that only 3% of employees surveyed admitted that they mishandled the company’s confidential information with malicious intent, while 24% said they just wanted to get their job done and 18% said they did not know they were doing something unsafe. Therefore, educating employees about how to properly protect confidential information is vital, especially in this era where employees are more mobile than ever and store or access their employers’ confidential information from their personal phones, computers, flash drives, and cloud services.

A. Understanding What is a Trade Secret

There is a whole host of information that companies have spent time, money, labor, and other resources on to cultivate and which they consider secret. These include financial business information, customer contact lists, employee records, and other non-financial information. Companies often wish to protect all of the information they have created, obtained, or otherwise
stored. But in order to create a culture of confidentiality that may withstand legal scrutiny, it is important to understand what is considered legally-protectable confidential or trade secret data.

In 2016, the Defend Trade Secrets Act (DTSA) was enacted, which provides for civil remedies in federal courts for the misappropriation of trade secrets. Before the DTSA was enacted, employers could only seek relief under state law when their trade secrets were taken. Although almost all states have enacted some version of the Uniform Trade Secrets Act (UTSA), there was no uniform application for relief. The DTSA does not eliminate or preempt the various state trade secret rights, but it does provide employers access to federal courts “if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce.”

Unfortunately, even with the enactment of the DTSA, there is no bright-line rule that defines what types of information constitute trade secrets. The analysis requires a fact-intensive examination of, among other things, the type of information concerned and the means by which such information is developed, obtained, disseminated or used. Under the DTSA, a trade secret can be in any form, regardless of “how stored [even in a person’s memory], compiled, or memorialized physically, electronically, graphically, photographically, or in writing,” and the information can be of any type: “financial, business, scientific, technical, economic, or engineering information.” However, it is required that: (1) the information is actually secret, because it is neither known to, nor readily ascertainable by, another person who can obtain economic value from the disclosure or use of the information; (2) the owner has taken “reasonable measures” to maintain the secrecy; and (3) independent economic value is derived from that secrecy.

Therefore, when creating a culture of confidentiality, an employer must think about what reasonable measures it will undertake to maintain the secrecy of its trade secrets. There are no minimum required measures. Instead, courts will look at the employers’ actions and on the economic circumstances surrounding the company and industry. But obviously, the more security measures that are implemented, the more likely that a court will find that the employer’s measures were “reasonable” and find that the claimed trade secrets deserve legal protection.

B. Onboarding Strategies

According to the 2017 Dell-End User Security Survey, nearly three out of four (72%) of the respondents said they would share sensitive or confidential company information under certain circumstances. The most common circumstances were: being directed to do so by management (43%); sharing with a person specifically authorized to receive it (37%); determining that the risk to the company is very low and the potential benefit high (23%); feeling it will help them do their job more effectively (22%); and feeling it will help the recipient do their job more effectively (13%). The survey noted, however, that in many of those circumstances, the employee independently made the judgment call on whether to share the confidential information. Therefore, it is imperative that employers create a culture of confidentiality from the start of the employment relationship. This culture can be created and maintained throughout the employment by taking the following actions:

- Have confidentiality policies and/or non-disclosure agreements that plainly state the company’s culture of confidentiality and the employees’ role in maintaining that culture. Employees must understand that they have an obligation to safeguard the company’s sensitive, confidential, and/or trade secret information and that there may be consequences if they fail to do so. Employees should sign
an acknowledgement that they have received and understood the policies or agreements, as well as stating that they know they must contact their manager or human resources if they have any questions or concerns. Employees also should be instructed regarding to which supervisors or managers they can report violations of the confidentiality policies.

- In addition to providing the confidentiality policy or non-disclosure agreement to a new employee for review and signature, time should be spent during the onboarding process to discuss the policies and the company’s expectations. This will further stress the importance of confidentiality to the new employee.

- Training and acknowledgement of the company’s confidentiality policies should be undertaken on a regular basis with all employees. Refresher courses on how confidential and/or trade secret information should be handled will serve to reinforce this culture of confidentiality. This training should include an explanation of the circumstances when confidential information may be shared and with whom. Employees should also be told to protect unauthorized access to the company’s systems by not using public Wi-Fi to access the company’s confidential information. They also should be instructed to not use public cloud services such as Dropbox, Google Drive, or iCloud for sharing or backing up their work, and they should not use their personal accounts to access those cloud services. Employees should also be reminded of such commonsense practices such as not leaving confidential information on desks, printers, garbage cans, or flash drives where others could view, download, or copy such information.

- Protect sensitive, confidential, and/or trade secret information with passwords and other security protocols to prevent unauthorized access, and encrypt the data when this information is in transit. In addition, monitor or track who is accessing this information.

- Make sure employees are only given access to the confidential and/or trade secret information that they actually need to do their work. Companies should have an inventory of their confidential and/or trade secret information and consider implementing a tiered system, so only certain employees have access to only certain information. Not only will this help prevent the unauthorized disclosure of confidential information, but it will also help an employer know which confidential information employees could have in their personal possession when they leave the company. Common examples of confidential information that should be inventoried are: client/customer lists; information about clients (e.g., pricing information, buying habits, preferences); business or commercial plans, including marketing strategies and infrastructure organization; research and development; formulas, designs and concepts; profit and loss statements; and competitor research.

- Consider workplace surveillance and/or monitoring of employees’ computers for suspicious activity, such as forwarding of company documents to personal email accounts. Radiant Global Logistics, Inc. v. Furstenau is a cautionary tale. In that case, the employer learned only after its office manager resigned and started working for a competitor that he had forwarded 300 emails to his personal account during the eight months prior to his resignation. Those emails contained the company’s financial forecasts, budgets, profit and loss statements, profit
margin data, customer lists, customer reports, and employee salaries. The company may have been able to avoid or minimize this loss of data if the office manager’s emails had been monitored throughout his employment. Be sure to seek the advice of legal counsel to make sure the surveillance and/or monitoring is done legally, as written consents or notices may be required.

- When an employee has not complied with the company’s confidentiality policy or procedures, immediate action should be taken to correct the behavior with the employee. This may include counseling or discipline to stress the importance of maintaining confidentiality, as well as an assessment of what steps should be taken so that this breach of confidentiality does not happen again.

C. Offboarding Strategies

Employees who leave their employers often take confidential and/or trade secret information. According to the 2017 Dell End-User Security Survey, over one-third (35%) of the employees surveyed admitted that it is common to take company information after leaving their employer. Implementing the onboarding strategies above should go a long way toward stopping this abuse, but employers should also take the following actions for departing employees:

- After employees give notice of their resignation and before employees leave the company, employers should monitor their email traffic and computer access for unusual activity. The employer’s policies should make clear that it is permitted to review employee’s personal emails if the employee accesses them on an employer issued device or computer. Often departing employees forward company documents that they or others have worked on, as well as customer contact or other company lists, to their personal email or onto flash drives. Also consider terminating resigning employees’ access to confidential information if they do not have a need for such information during their notice period.

- After employees have left and before their laptops are reissued to other employees, employers should examine the departing employees’ computers to see if any unusual activity can be found.

- Take the time to conduct exit interviews with departing employees. Not only should the interviews cover topics such as the employees’ experiences with the company and the reasons for leaving, the interviews should also go over the employees’ access to and return of all confidential information, the equipment they used for work (including their own devices) and/or other non-company digital spaces such as cloud-based storage, external email servers, social media, and external equipment (e.g., flash drives). Any confidentiality, non-disclosure or other agreements (e.g., non-competition and non-solicitation agreements) should be discussed during these exit interviews also.

- Consider having employees sign a short statement affirmatively acknowledging that they have returned all company property (including confidential information) and not retain any confidential information (including in their personal emails).

- After employees resign or are discharged, be sure to immediately terminate their access to the company’s systems, to ensure there is no opportunity for them to download or access any data remotely.
• Contact vendors and/or customers to let them know that the former employee is no longer the company’s contact.

• Obtain all of the company’s property from the ex-employee and follow-up with the former employee when they fail to return the property right away. Employers may want to provide employees with a convenient method of returning equipment and data, as well as obtain a certification from ex-employees that all of the company’s property has been returned.

• If an employee signs a severance agreement, be sure to include either a reaffirmation of the confidentiality agreements he has already signed or include new confidentiality polices in it. Be sure to state that these provisions in the severance agreement are material, which helps to reinforce the important of same.

• If an employer is concerned about a particular ex-employee, it may send a reminder letter to him that outlines the confidential policies he has signed and informs him that it will continue to monitor the situation. If an employer suspects that an ex-employee, in fact, has taken and/or is using the company’s confidential and/or trade secret information, the employer may decide to send a cease and desist to the former employee. If the ex-employee could use such information with a new employer, then it may be appropriate to also send a cease and desist letter to the new employer.

D. Conclusion

Creating a culture of confidentiality does not just happen. It requires planning, action, and continual follow up. Companies make huge investments in cultivating their trade secrets, and it is important that they also make the necessary investments to protect those trade secrets from being misappropriated. The strategies above from onboarding to offboarding will help companies create that culture of confidentiality to hopefully avoid the loss of trade secrets and/or costly litigation.
ENDNOTES


6 Association of Certified Fraud Examiners, Report to the Nations 2018 Global Study on Occupational Fraud and Abuse.


8 18 U.S.C. § 1839(3).


Creating a Culture of Confidentiality From Onboarding to Offboarding

Presenters
Heidi K. Durr (St. Louis) and David P. Thatcher (Atlanta)

Moderator
Adam Dougherty (Dallas)

Overview
- Onboarding
- Midstream
- Offboarding
Onboarding: Pre-Employment

- Conduct a careful analysis of your company’s confidential information and trade secrets
- No two companies are the same, but many confidentiality policies are

Onboarding: Pre-Employment

- What is a trade secret?
  (1) the information is actually secret, because it is neither known to, nor readily ascertainable by, another person who can obtain economic value from the disclosure or use of the information;
  (2) the owner has taken “reasonable measures” to maintain the secrecy; and
  (3) independent economic value is derived from that secrecy
Onboarding: Pre-Employment

- Starts before the employee’s first day of employment:
  - Offer letter
  - Determine if the individual is covered by a former employee’s restrictive covenant

Onboarding: First Day

- Maintain a checklist
- Facilitator discusses the policy, checks boxes, dates, and signs it
- File the checklists
Onboarding: First Day

- Onboarding
  1. Stand-alone confidentiality policy
     - Include specific examples of confidential information and trade secrets
     - Signed acknowledgment
     - Non-compete and/or non-solicitation agreements

- Onboarding
  2. Handbook
     - Confidentiality policies
     - Signed acknowledgment
Onboarding: First Day

- Onboarding
  3. Job Description
  - Maintaining confidentiality is an essential function
  - Signed acknowledgment

Boots on the Ground

- Reasonable steps to maintain secrecy or confidentiality
  - Designating material as trade secret or confidential
  - Segregating and inventorying valuable material
  - Restricted access to valuable material
    - Identifying necessary individuals
    - Limiting methods of access
  - Restrictions on copying and distribution
Boots on the Ground

- Risk Management Practices
  - Registry of trade secret or confidential information
  - Identify potential risks
  - Analyze likelihood of various risks
  - Plan and develop plan to address those risks
    - Review and update this plan regularly

- Identifying potential risk areas
- Use of technology to secure data
- Use of technology to identify misappropriation
Boots on the Ground

- How do you identify your company’s critical data?
- What is your organization doing to ensure access for necessary employees, but preventing others from accessing?

Critical steps to proactively managing risks

- Know where your company’s high-value/high-risk information resides
  - Enterprise servers/network drives
  - Local drives, cloud storage
  - Email, social media, etc.
- Know who has access/ability to disable
- Prepare a decision matrix to guide preservation approach and ensuing actions
Boots on the Ground

- Decision matrix considerations
  - Employee’s current/former positions with company
  - Relevance of material to which they had access
  - Security level of material
  - Subject to legal or regulatory hold
  - Type or significance of the matter

Boots on the Ground

- Preservation actions differ by system or technology, but may include?
  - Issuing a legal hold
  - Preserving in place
  - Collecting to preserve
    - Active data collection or forensic image
Boots on the Ground

- Protections
  - Limit ability to store data on local devices
    - Especially PST files
  - Ensure mobile devices utilize remote management
    - Allows company to remove data remotely
  - Assess whether remote access software installed
    - Used to access the computer or your network

Offboarding Strategies

- Over one-third of employees surveyed admitted it is common to take company information after leaving their employer.*

*2017 Dell End-User Security Survey
Offboarding Strategies

- After employees give notice of resignation and before they leave, employers should monitor their email traffic and computer access for unusual activity.

- Do an exit interview.
- Review access to and return of all confidential information.
- Review equipment used for work and/or other non-company digital spaces (e.g., flash drives).
- Review any confidentiality, non-disclosure, or other agreements.
Offboarding Strategies

- Examine employee’s computer before it is reissued to another employee.

- Do not forget to terminate employee’s remote access to the company’s systems.
- Tell vendors and/or customers that former employee is no longer with the company.
- Consider sending cease and desist letter to former employee and/or new employer.
Creating a Culture of Confidentiality From Onboarding to Offboarding

Presenters
Heidi K. Durr (St. Louis) and David P. Thatcher (Atlanta)

Moderator
Adam Dougherty (Dallas)