Your Employee is Leaving…. How Do You Safeguard Your Company's IP?

Matthew C. Luzadder

March 2, 2017

It is a fact: employees leave. According to the Bureau of Labor Statistics, the average worker currently holds ten different jobs before age forty.[1] Because employee transitions are inevitable, businesses must prepare to secure their data when an employee exits the company. Otherwise employers risk having their information (e.g., customer lists and related information, research and development, and strategic business development) stolen. Stolen information can lead to the loss of competitive advantage, embarrassment and devaluation of image and goodwill, reduced profitability, and loss of core business technology. These types of damages are difficult to ascertain in monetary terms.

Data is protected by (1) common law, (2) statutory law (e.g., Uniform Trade Secrets Act, Economic Espionage Act, Computer Fraud and Abuse Act, and state criminal codes), and (3) contractual agreements (e.g., non-compete, non-solicitation of clients). While the law protects your data, a lawsuit to enforce such protection can be costly and time consuming with uncertain outcomes. Thus, preemptive planning is the best defense.

Be aware of modern realities. Fewer employers provide phones, laptops, and tablets to their employees. More employers are expecting employees to bring-your-own-device ("BYOD"). In 2015, only 15% of mobile equipment and service is all corporate owned and supported.[2] With increased electronic access to proprietary information on personal devices, it is not difficult to imagine the ease in which information may be taken, both by deliberate actors and through inadvertent acts. The risks associated with BYOD can be alleviated with proactive planning and comprehensive policies and procedures. Consider implementing the following into your BYOD policies and procedures.

1. Reserve broad rights, within legal limits, to examine personal devices.
2. Consider requiring an employee's authorization for the company to audit and wipe/reset upon separation.

3. Require employee's signed acknowledgment of compliance with data security measures upon separation.

In today's world, employers must act to reinforce the notion that: "This is the Company's intangible / intellectual property. The Company has an affirmative right to ensure it is being used in accordance with established policy." This approach puts the onus on the employee to protect all the company's data wherever it is located.

The checklist below provides a guide employers can use to create their own internal process.

1. Understand that one of the great threats are current and former employees who know how and where information is stored, and the details on the creation or use of trade secrets.

2. During the interview process, you should think about proposing and bargaining over restrictive covenants in the employee's contract. Because Courts will only enforce "reasonable" restrictive covenants, construct the restrictive covenants as narrowly as possible.

3. Train your employees. Employees should understand what information is confidential and considered a trade secret. Be specific when you define the "trade secrets" you seek to protect. In the absence of training, people may make incorrect decisions based on their assumptions. Make it easy to do the right thing.

4. Maintain information on employee access. Information Technology ("IT") should maintain a document that lists each employee's access to the company's information systems. This will allow IT to disable all of the access rights promptly and managers to collect all devices from the departing employee.

5. Conduct an Exit Interview. Remind employees that company information is confidential and should not be revealed to an outsider. Review document retention requirements including the process the employee used for saving electronic or print documents, discuss any company devices that need to be returned, and review any company related accounts they access. This provides individuals with notice of their obligations and establishes the basis for pursing individuals who may intentionally or unintentionally retain property information that could be used outside of an organization after employment.

6. Treat the employee with dignity as she is leaving. Be reasonable and respectful. People are more likely to make poor decisions when they feel mistreated.

If you have specific questions about drafting policies, procedures, or restrictive covenants, please reach out to one of our labor and employment attorneys.

[1] https://www.linkedin.com/pulse/how-many-jobs-average-person-have-his-her-lifetime-scott-marker

[2] Cass Information Systems, Inc., the Cass 2015 BYOD & Mobility Study