Combatting Corporate Espionage In The Digital Age

Insights
3.06.18

In the modern age of relatively cheap and ever-evolving technology, corporate espionage is a real threat that could be perpetrated by any employee or other insider at any time. The term "corporate espionage" covers many different types of behavior, ordinarily taking the form of a malicious company insider secretly stealing confidential company information, usually for use in a competing business. The insider may be planning on joining an existing competitor, or may be planning on founding a new competing business of their own. In essence, however, the term refers to any act of spying that is carried out for commercial purposes. Regardless of the form it takes, the wrongdoer will be looking to exploit the time, money, and hard work you have put in to make your business successful for their own malicious purposes.

Corporate espionage comes in many forms, some more sophisticated than others. While there is no foolproof way to spot all transgressions before it is too late, here are some general warning signs to watch for:

- The employee begins working from home or out of the office more often;
- You see an increase in after-hours work or unusual office or remote computer access;
- The employee begins meeting with customers without recording meetings in company systems;
- The employee knows about business matters they are not directly involved in;
- The employee becomes disgruntled or has a sudden change in attitude;
- Files or other materials are missing from the office with no explanation;
- The employee unexpectedly resigns without advance notice; and
- The employee refuses an exit interview or does not want to discuss post-resignation employment plans.

While not necessarily indicative of any improper actions, any of these behaviors should be considered "red flags" that merit further investigation or research.

To mitigate the risks of corporate espionage, some companies choose to invest in computer software that can detect certain activities that may not be outwardly obvious. These programs can be configured to monitor and detect common actions such as:

- Outgoing email sent to personal email addresses;
- File uploads to dropbox or other FTPs;
- External media such as flash drives or external hard drives accessing company files;
- Improper access to restricted confidential electronic files; and
- Irregular electronic access, such as excessive and unnecessary review of records containing customer contact information.

If you have any suspicions about a departing employee's motives, it is absolutely critical not to reissue the departing employee's electronic devices to other employees. You could risk losing objective computer evidence showing that the departing employee used the device for an act of corporate espionage. In such a situation, you may want to consider preserving a forensically sound image of all machines used by the employee.

Many types of business information are vulnerable to acts of corporate espionage if not adequately protected. These include, but are not necessarily limited to:

- Customer information – Your customers are likely your most valuable asset, and the asset that could harm you the most if it disappeared.
- Business process information – This unique information is often the result of years of effort and countless sums of money. Your competitors want to know how you do what you do, so they can try to do it better or cheaper.
- Intellectual property – Chances are you have invested large sums of money in your intellectual property portfolio. Confidential information related to your intellectual property could be very valuable to a new business or a competitor that is actively trying to take your market share.
- Financial information – This information could be used to harm your company in many different ways.
- Bidding/pricing structures – Your bidding or pricing structure says a lot about your business. Your competitors want to know this information so they can try to undercut you.
- Employee information and demographics – This information may not be ordinarily thought of as confidential, but it can be very valuable depending on the extent of what is taken.
- Other industry specific information – Every business has valuable information that is valuable in its particular industry that may not be recognizable as valuable outside of the industry. Chances are the wrongdoer knows about this information and could be looking to exploit it.

Corporate espionage is an unfortunate reality of modern life. By knowing some of the warning signs and the types of information that are vulnerable, you may be in a position to put a stop to an espionage attempt before it is too late.