# The Legal Strategist

S. Barrett P.C.

WWW.SBARRETTLAW.COM

Fourth Quarter 2017

There is a common misconception about corporate espionage: many view the practice as a concern for only businesses with sensitive, government-related intelligence dealings. But this could not be further from the truth. Small businesses, large corporations and even some individuals are victims to such stealthy acquisition of information. It is projected that American companies, as a whole, lose anywhere from 1 billion to 10 billion annually due to corporate espionage. This loss is extreme, but easily preventable. A general lack of acknowledgement coupled with small oversights leads to the all-too-easy theft of critical information. Corporate espionage is rarely publicized when it occurs, but that doesn't mean it's nonexistent.

The Feature Topic is a cursory review. If you would like more information on this, or any other topic previously covered in our newsletter, which can be viewed on *The Legal Strategist* tab of my web site, please contact my office at 713.526.1883.

Scott Barrett

### Texas Esoteric Facts

The San Jacinto Monument in LaPorte, TX is listed as the tallest stone column memorial structure in the world, 15 feet taller than the Washington Monument in Washington, D.C

## Feature Topic: FIGHTING CORPORATE ESPIONAGE

When it comes to protecting a company from economic espionage or data theft, business owners don't need to hire James Bond for protection, nor Ian Flemming for ideas. Generally, just having the right policies and security measures in place is all a company can do without making significant sacrifices to the movement of information and exchange of ideas.

However, when a company's process or data is so confidential that disclosure to a competitor could cause disruption, significant sacrifices may actually be worthwhile to safeguard the information. Here are some tips on how to protect against corporate espionage.

1. Cyber Security. If you got something worth protecting, then protect it in real life and online! Just like individual consumers, with each passing day, businesses are becoming more reliant on technology and internet connected devices. As such, ensuring that sensitive data is secured against online attacks is critical. Additionally, it may be necessary to have specific procedures or software for your own employees that would prevent your own employees from stealing the data, or even accessing the data on a non-company owned device. Finding the right balance is different for every business.

2. No Nonsense NDA. Having a strong Non Disclosure Agreement (NDA) might have a few inhibiting factors, or potentially drive up costs. However, when it comes to protecting intellectual property, strong, enforceable NDAs are essential.

3. Shred Sensitive Documents. Since a majority of information stolen is in the physical form, companies should shred all documents before they are discarded. A regular shredding process will prevent essential company information from being stolen from the company.

4. Avoid Printing Proprietary Information. Do not print sensitive company information unless it is absolutely necessary. Then immediately place the information in a secure envelope or place until it reaches the intended party. Information lying around on a desk may be easily copied, photographed, or stolen. Companies should change their policies in order to prevent this occurrence.

5. Physical Security. Secure all necessary printed documents in a locked file cabinet. Keep the cabinets locked when the cabinets are not in use. This prevents employees or other parties from stealing documents or copying documents.

6. Preventing Computer Espionage. Trojan Horses and viruses are often used to lift information from corporate individuals. This type of espionage is very targeted and covert. Computer hackers have developed elaborate Trojans to prevent corporations from determining the origin of the hacker. The hackers also guard against spy program removal and from detecting that the program exists by circumventing any virus software. Corporate hackers use the information to provide directly to a competitor or to convince corporations to purchase their software to prevent future attacks. The latter occurrence is akin to blackmail. Information may also be shared to the very individuals you are entrusting to keep you protected. Individuals who purchased anti-Trojan or anti-virus software must trust the individuals in the corporations employed to protect them, because that company may also be guilty of corporate espionage. Anti-virus developers may hack a system faster than any outside entity.

7. Protect Servers. Servers should only be accessed by trusted IT professionals. Servers should be stored offsite or be stored in locked cabinets that cannot be accessed by normal means. The cabinets should be able to withstand heat and cutting tools. Employees should be sure their computers are free of keystroke gathering technology when working from remote locations on web based applications.

If you would like more information on how to develop company policies and procedures to protect your company's sensitive data, please contact Scott Barrett to set up a consultation.