Trade Secrets Protection in the Digital Age: What Every Business and Entrepreneur Needs to Know

For start-ups and early-stage companies, who may or may not have their technology and information protected by patents, often it's their trade secrets which are their most valuable intangible assets, and which help to differentiate them from others in the marketplace.

Unlike patents, which confer upon their owners exclusive rights to exploit their technologies and inventions for a fixed period, trade secrets afford (potentially for eternity) protection against breach of confidentiality or acquisition by improper means, such as theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage. To enjoy legal protection, however, a trade secret must remain a "secret." Any public disclosure or use of such information, even without the knowledge or consent of the owner, destroys the "secret," both legally and practically speaking. In other words, once the genie is out of the bottle (either because of independent development, reverse engineering, or disclosure where no duty of confidentiality existed), the protected status of a company's trade secret is lost (and lost forever), and others are free to make use of such information.

Given the growth in new technology and the relative ease in which data can be downloaded and transferred, protecting trade secrets in this digital age has become increasingly more challenging. As there always lurks a miscreant (rogue employee, unscrupulous competitor, hacker, or industrial spy) ready to abscond with your corporate "jewels," often stolen with a simple click of a mouse, companies now more than ever should implement strong trade secrets security programs to protect their most prized informational assets.

This post outlines important legal requirements and best practices companies should consider to help preserve the protected status of their trade secrets in the digital age.

What Are Trade Secrets?

"Trade secrets" are generally defined as confidential proprietary information that provides a business with a competitive advantage or economic benefit. Trade secrets are protected under the Economic Espionage Act of 1994 ("EEA") at the federal level, and 48 states (plus Puerto Rico, Washington, D.C. and the U.S. Virgin Islands) have enacted statutes based upon the Uniform Trade Secrets Act ("UTSA"), a model statute designed to unify trade secret law across the United States. (Massachusetts and

New York are the only holdouts, although there is currently a Massachusetts UTSA bill pending in the legislature. Trademarks are protected in these jurisdictions as a matter of state statute and common law.)

Under the UTSA, to be protectable as a trade secret, information must satisfy the following requirements (each of which will be discussed in greater detail below):

- the information must fall within the statutory definition of "information" eligible for protection
- the information must derive independent economic value from not being generally known or readily ascertainable by others using appropriate means
- the information must be the subject of reasonable efforts to maintain its secrecy

Determine Which Data Constitutes Trade Secret "Information"

The UTSA (and corresponding state statutes) generally define "information" to include:

- All forms and types of financial, business, scientific, technical, economic, and engineering information
- Patterns, plans, compilations, formulas, designs, prototypes, methods, techniques, processes, procedures, and computer codes
- Information that has commercial value, such as customer lists or the results of expensive research.

The types of information that constitute protectable trade secrets are essentially limitless. Indeed, courts have interpreted trade secret "information" to cover virtually any commercially valuable information used to conduct business that is protected from public disclosure, including chemical formulae, research results, pricing and marketing techniques, manufacturing processes, pricing data and figures, product compositions and designs, confidential costs, internal market analyses and forecasts, and customer lists.

"Economically Valuable" and "Not Readily Ascertainable" Information

To qualify as a protectable trade secret, the information must derive independent "economic value" — actual or potential — from not being generally known to and not being "readily ascertainable" by others. A trade secret's value generally is not the information itself; rather, it resides in the fact that others (principally a company's competitors) do not possess the information and are therefore not able to put the

information to use for their own benefit.

In determining whether information qualifies as a trade secret, courts generally consider whether:

- Reasonable measures (not all conceivable efforts) have been put in place to protect the information from disclosure
- The information has actual or potential commercial value to the company or provides the company with a competitive advantage
- The company devoted significant time, money and other resources to develop the information
- The information is known by a limited number of people *(i.e.,* employees and other parties in a "confidential" relationship with the company) on a need-to-know basis
- The information would be useful to competitors and would require a significant investment of time, expense or effort to duplicate or acquire the information
- The information is not generally known to the public, or to other persons or businesses outside of the company who can obtain economic value from its disclosure

Implement Reasonable Measures to Maintain Secrecy

The most important criterion in determining whether something qualifies for protection as a trade secret is whether it is indeed secret. Businesses should therefore implement technical, administrative, contractual and physical safeguards to keep secret the information sought to be protected. As relative, not absolute, secrecy is required, businesses should take reasonable measures under the circumstances to prevent their trade secret information from being misappropriated or disclosed. These measures should be tailored to the day-to-day business of the particular enterprise, the nature of the confidential information sought to be protected, and the risk of harm to the business in the event of misappropriation or disclosure (inadvertent or otherwise).

Administrative Safeguards to Protect Your Company's Trade Secrets

Conduct a Trade Security Audit: As an initial step, companies should conduct an internal trade secret audit to identify information that should be protected as a trade secret, where it is located, with whom it needs to be shared, and the steps that are being currently taken to protect it from disclosure. Audits should thereafter be conducted on a regular basis to assess the efficacy of existing security

procedures and to identify any new threats or program deficiencies.

Draft a Trade Secrets Policy: Companies should adopt a trade secrets policy that: (i) defines what constitutes the company's trade secrets or confidential information; (ii) specifies the steps to restrict access to confidential information (check-in and check-out procedures, use of "confidential" legends on documents, etc.); (iii) explains the procedures under which information may be disclosed to approved third-parties; (iv) reproduces the material terms of any restrictive covenants; and (v) outlines the company's computer and telecommunications security procedures (*e.g.*, passwords, encryption, etc.). The trade secrets policy should also include specific provisions addressing social media and e-mail (for example, that any e-mail, instant message, or social media post that passes through a company computer, server, device, or equipment is considered company property and may be monitored; that employees are prohibited from forwarding any company document, data, or information to an outside e-mail account without prior supervisory approval; and that employees may not disclose confidential company information on any blog, chat room, or other social media site.)

Require Written Acknowledgments: Employees should be required to sign a written acknowledgment that they have reviewed and understand the company's trade secret policies and their compliance obligations.

Share Information on A "Need-to-Know" Basis: Restrict access to trade secret information on a business-need-to-know basis, and compartmentalize the information so that only the portion that the employee requires to do his or her job is revealed. With this in mind, there is probably little reason to grant HR access to a manufacturing formulae or your marketing department with your company's executive compensation schedule. Generally speaking, only a few key employees should have access to all of a company's trade secret information.

Secure Contractual Protections: A company's employees, licensees, vendors, suppliers, contractors, subcontractors, consultants and potential business partners should be required to commit in writing not to use for their own benefit or disclose to others any company trade secrets to which they may become exposed, except upon the prior written consent of the company or as required by law. In addition to such confidentiality and non-disclosure agreements, companies should also consider having their employees sign an assignment of invention or work, which assigns to the company all of the employee's rights in any inventions or new discoveries made by the employee during the course and scope of his or her employment.

Assign Unique Employee Identifiers: Each employee with computer access should be assigned a unique identification number to enable system tracking. Restrict employees' access to computer files that are unrelated to their work.

Label Trade Secret Information: Clearly label all trade secret information to identify it as such (for example, "Confidential: For Internal Use Only" or "Proprietary and Trade Secret Information"). Similarly, computer files and databases should include a legend alerting employees that the information contained therein constitutes the employer's trade secrets. These designations should be periodically reviewed and updated as necessary. Avoid overuse of trade secret labels to prevent diluting the strength of such marks.

Conduct Employee Training: Train your employees and new-hires about information secrecy, the company's security policies and procedures, and the proper procedure to respond to theft of trade secrets. Issue periodic reminders about your employees' security responsibilities and secrecy obligations. The policies should be reinforced by including them on start-up screens that are accessed each time an employee logs in to the employer's computer or network.

Entrance Interviews: New employees with knowledge of a former employer's trade secrets may expose the new employer to liability by using or disclosing secrets in the course of their employment. Entrance interviews for new hires should be conducted, therefore, to determine whether they are subject to a duty of confidentiality or covenant not to compete with their former employers. New hires should also be advised not to utilize or disclose any information or materials belonging to another company, particularly technical and business information that was protected as confidential.

Exit Interviews: Conduct exit interviews with departing personnel to: (i) remind the employee of his or her continuing duty not to use or disclose trade secrets, and review any documents to that effect; (ii) recover all keys, badges, security passes, computer disks, laptop computers, USB thumb drives, PDAs, smartphones, and other digital or electronic devices issued by the company; and (iii) require the departing employee to sign a statement confirming that he or she: (a) has returned all company materials (including all copies); (b) has deleted all confidential and trade secret information from the hard drive of any computer or digital or electronic storage devices he or she may have used; and (c) understands and agrees to abide by their continuing obligations to maintain secrecy.

Disable Accounts of Departing Employees: Companies should immediately disable the accounts and access privileges (including remote

login) of any employee who is terminated or resigns; their passwords and remote access codes should also be changed. Companies should also consider requiring those to whom they provide access to trade secrets to agree not only to return all such secrets at the termination of the relationship, but also to delete them from the hard drives of any computers or digital or electronic storage devices (including USBs and similar devices) not owned by the company that they may use.

Post-Departure Investigation: Following an employee's termination or resignation, companies should conduct a thorough computer audit, including searching for information downloaded or copied from employee's laptops, smartphones, Internet browser cache, cookies, firewall logs, and all the places where e-mail might be stored, and all contact manager files. A thorough computer forensic analysis should be performed in the event trade secret misappropriation is detected or suspected.

Technical Safeguards to Protect Your Company's Trade Secrets

Encrypt Data: All confidential information that is stored and transmitted across open, public networks should be encrypted.

Technical Restrictions: Limit access to confidential information through passwords and network firewalls. Require employees working remotely to utilize secure connection platforms, such as remote desktop software, to prevent them from downloading company information to their laptops or personal devices.

Use Firewall and Antivirus Software: Install and regularly update firewall and antivirus software on all company computers and devices connected to the internet.

Develop a Password Policy: Develop a password policy for all employees with access to confidential information, requiring them to select secure passwords (using both letters and numbers), change their passwords on a regular basis (*e.g.*, every 60 days), and avoid reusing old passwords or vendor-supplied default passwords.

Catalogue Data Access: Monitor and log all employees' internet activity, and access to network resources and confidential information.

Monitor Downloads and Emails: Monitor large downloads and emails with sizeable attachments to help detect potential theft of confidential information. Also, prohibit employees from downloading company information to personal devices or sending such information through personal e-mail.

Prevent the Use of Unauthorized USB Drives: Companies may prevent the use of unauthorized USBs and similar devices by disabling USB ports on company computers.

Physical Safeguards to Protect Your Company's Trade Secrets

Surveillance: Install surveillance equipment (*e.g.*, closed-circuit TVs) to monitor entry into company facilities, access to servers and other critical systems, or removal of confidential information.

Physical Barriers: Trade secrets should be kept in areas that are inaccessible to the public, and file cabinets or offices where such information is maintained should be locked. Consider requiring key-card access for entry into restricted areas containing highly sensitive information.

Guards: Station uniformed security personnel at each facility entrance.

Signage: Post warning signs in areas near where confidential information is located to remind employees of their duty of confidentiality, and not to review any such information unless they have been specifically authorized to do so.

Limit Visitor Access: Visitor access of a company's plants and facilities should be limited. Companies should consider establishing sign-in procedures, issuing ID badges to all visitors entering the premises or secured areas, and requiring that all visitors be escorted by a company employee.

Ban Camera Phones: Camera phones should be banned from all areas that contain classified information.

Disposal: Shred all paper documents containing confidential information before trashing them, and be sure that all digital media is erased before being discarded.

Conclusion

Given the ease in which data can be stored, accessed, disseminated, and transported, it is little wonder that trade secret misappropriation is on the rise. Thousands of pages of a company's confidential information can be downloaded onto a flash drive, within seconds. Even an iPhone can be used to surreptitiously copy a company's trade secret information. Trade secret owners should take proactive steps to implement adequate security measures — administrative, technical, and physical — to properly mitigate against these enhanced risks. As both a practical and legal matter, trade secret protection measures must constantly evolve to address the risks inherent in new technologies. Staying even slightly ahead of the changing times is your best bet for protecting your informational assets (and competitive edge).

If you have any questions about this article, please contact:

Robert McHale, Esq.
R | McHale Law
9 West Broadway, Suite 422
Boston, MA 02127
Tel. 617.306.2183
Email: robert.mchale@rmchale.com