Keep On The Right Side Of The Line:

A Trade Secret Law Perspective

By Michael Wexler and Robert Milligan, Seyfarth Shaw LLP

An episode of NBC's *The Office* earlier this year provided an amusing yet distressingly realistic illustration of the ease with which a company can inadvertently disclose its most sensitive business information. The episode involved two employees of the fictional paper company Dunder Mifflin – Michael Scott and Dwight Schrute – who were tasked by their company's CFO to learn about a competitor, Prince Paper. In an effort to obtain the information, Scott and Schrute slyly posed as a potential client and a potential new employee, and went to Prince Paper's office to ask seemingly innocent questions about the company. Unaware that he was freely and readily giving away his company's valuable secret information to a competitor, Prince Paper's principal disclosed sensitive information and he even went as far as to provide a customer list.

The episode from *The Office* illustrates the pitfalls when a company does not do enough to protect its key information. Companies must continuously and aggressively seek new and effective ways to protect their proprietary and trade secret information. If a trade secret is leaked, its value to the company may be severely compromised and lost forever. Likewise, to avoid the often detrimental and serious repercussions that accompany improper intelligence gathering, companies must be extremely vigilant to ensure that they use only ethical means to acquire information about their competitors. Competitive intelligence (CI) professionals must play both offense and defense in order to gather useful information in an ethical manner while simultaneously protecting their own companies from disclosing sensitive information. This article addresses some best practices for CI Offense and CI Defense.

THE ROLE OF COMPETITIVE INTELLIGENCE

Competitive intelligence is a business function that companies utilize for the purpose of gathering and analyzing useful information about competitors *in an ethical manner.* CI professionals also serve to help protect their company from leaking the company's own sensitive information to competitors. Particularly in today's economic climate, CI professionals need to be mindful that only intelligence that is gathered lawfully truly benefits their company in the long run.

There may be a temptation to push the envelope or take unnecessary risks to distinguish oneself or one's company in these economic times. However, recent cases involving the theft of trade secrets, including the recent prosecution of a former engineer for economic espionage to benefit a foreign country, serve as a stark reminder that CI professionals should do it right or not do it all. With the pressures existing in our economy, companies and CI professionals cannot afford

to take lightly the obligations imposed upon them under the law. In the long run, companies that gather intelligence ethically will benefit from the fruits of lawfully obtained information and eliminate the significant risks that come from crossing the line.

TRADE SECRET THEFT AND ITS CONSEQUENCES

Those who engage in improper intelligence gathering run the risk of exposing themselves and their companies to claims of trade secret misappropriation and other legal claims. Trade secrets consist of proprietary information that is:

- not generally known
- valuable because its economic benefit is derived from its secrecy
- subject to reasonable efforts to protect its secrecy

Common trade secrets include tangible customer lists, know-how, formulas, manufacturing processes, marketing strategies, sensitive financial and pricing information, unique software and source codes, and specialized knowledge about customers. The formulas for Coca Cola and WD-40 and the recipe for KFC are common examples of trade secrets. Trade secrets may be found in a variety of locations including lab notebooks, computer files, databases, drawings, rolodexes, whiteboards, e-mail, or in one's head. Trade secret thieves may include former employees, foreign competitors, on-site contractors, domestic competitors, and current employees. They might copy documents, download or e-mail information from computers, or memorize information. If discovered, these individuals can face civil and criminal penalties.

The destructive consequences of improper intelligence gathering are real. The engineer discussed above was

SIDEBAR 1: BEST PRACTICES FOR GATHERING INTELLIGENCE

Obtain information freely, honestly, and always act in an ethical manner. Always identify yourself and who you are with prior to conducting interviews. If information is obtained dishonestly, not only will your ability to use the information be compromised, but the information may be subject to further legal action.

Avoid the use of any deceit and false identity. Never take information under false pretenses as described in *The Office* example. False pretenses may make the acquisition of the information easier, but the information will be useless and the employees and companies that use such methods may face serious consequences when the unethical measures are later discovered.

Don't wiretap, hack, bug, spy, bribe, or blackmail to obtain CI. The use of any of these methods is unethical and the information obtained will be unusable. Such improper intelligence gathering will subject your company to legal claims and possible punitive damages.

Rely on public sources of information. The internet, libraries, and trade shows can provide a wealth of useful information. Relying on public information will ensure that the information was gathered in an ethical manner and will protect against claims of trade secret misappropriation.

Before using any information from public court filings, make sure that there are no protective orders in place in the case that may cover the information.

If you have suspicions about the source and accuracy of the information, err on the side of caution before using the information and consult legal counsel. Do not assume that the information was obtained through ethical means if you are uncertain. Such an assumption may destroy the value of the information. This is particularly true of information found on the internet from unreliable sources or sources that may be intentionally or recklessly attempting to harm the company about which information is supplied.

Make sure your company's CI professionals are members of SCIP. This will provide them access to SCIP's Code of Ethics and literature and training about addressing ethical dilemmas. This will allow them to continuously refresh themselves on their responsibilities and obligations.

Companies should have clear and lawful intelligence gathering objectives and policies. Companies that have effective policies which foster the ethical gathering of intelligence will not need to or be tempted to gather information in an unethical manner and thereby will protect themselves from liabiliity.

Arm yourself with the law by consulting legal counsel. Employees that have a clear understanding of the line between ethical and unethical intelligence gathering practices will be less likely to mistakenly cross the line and subject their company to liability. This line must always be clearly identifiable to employees and must always be at the forefront of their minds when gathering intelligence.

Do it right or don't do it all. The third alternative, doing it wrong, will place the employee and the company worse off than they were if they hadn't done it at all. The desired information will lose its value to the company and the consequences that accompany unethical intelligence gathering practices could be detrimental.

SIDEBAR 2: BEST PRACTICES FOR SEALING LEAKS

Ensure that your company has education and training programs in place that educate employees about CI, what constitutes trade secret and confidential information, and the company's expectations of secrecy and confidentiality. This will help prevent employees from following in the footsteps of the Prince Paper employee from *The Office* and mistakenly disclosing confidential information.

Screen employees and third parties before providing access to trade secret and confidential information. Screening measures may include conducting criminal background checks, credit bureau checks, and finger printing, as permitted by applicable law.

Have employees and third parties sign confidentiality and nondisclosure agreements (NDAs) acknowledging their obligations to treat such information as secret. Have third parties, including vendors, business partners, and contractors, with access to such information, sign similar confidentiality and non-disclosure agreements.

Limit the availability of the trade secret and confidential information within computer systems. For example, use separate databases, separate computers and a variety of passwords in order to reduce accessibility. Keep hard copies of secret materials in a locked vault, safe, or cabinet.

Require a checkout procedure for trade secret and confidential information removed from the work area and attach electronic sensors to important trade secret documents. Maintain logs identifying trade secret and confidential information and mark such documents as confidential.

Do not leave trade secret and confidential information exposed or accessible to the public, e.g. on-line, publications, and trade shows. Ensure that your website is secure and that secret items have not entered the public domain.

Protect against unauthorized physical access to trade secret and confidential information. Utilize protection measures such as security systems, alarms, personnel, escorts, and visitor badges. Require identification of all persons seeking access.

Audit the files of high risk employees for the unauthorized possession of trade secret and confidential information. Also check high risk current and former employees' on-line public postings in social networks and other on-line forums for improper disclosure of trade secret and confidential information.

Be selective in what information is revealed to the public, especially at trade shows. Employees that attend trade shows should receive training in advance concerning the importance of keeping information secure. (See the Competitive Intelligence Foundation's book *Conference and Trade Show Intelligence*.)

Keep an eye on your company's government filings, e.g. SEC, court filings, etc., to ensure trade secret and confidential information is not disclosed. Monitor professional journals to ensure that trade secret and confidential information has not be disclosed by employees or former employees.

Consider hiring a security specialist and legal professional to conduct an audit of your company's trade secret protections. The trade secret audit should identify and classify the company's proprietary information and assess the current protection measures in an effort to implement an effective and efficient trade secret protection plan.

Work with your company's IT, Security and IP Departments to protect company's assets. Have a written trade secret protection plan and follow the plan. The trade secret protection plan should aim to reduce the risk that trade secrets will be improperly disclosed or accepted by the company, provide evidentiary support in the event that legal action for trade secret theft becomes necessary, and limit the risk of claims of misappropriation by other companies.

convicted of six counts of economic espionage and will now likely spend the rest of his life in jail, as each charge of economic espionage carries a maximum possible penalty of 15 years in federal prison and a $500,000 fine. In a recent study commissioned by McAfee, researchers polled 800 executives at businesses with more than $250 million in annual sales. Of the executives surveyed, 42 percent said that laid off workers were the biggest threat to businesses caused by the current recession. (McAfee's Unsecured Economics Report 2008 is available at http://resources.mcafee.com/content/NAUnsecuredEconomiesReport.)

McAfee's researchers estimate that data theft cost businesses $1 trillion in 2008 and businesses reported losing $4.6 million on average in 2008 as a result of data theft. Further, a national communication company recently received a multimillion-dollar damage award and an additional $7 million in punitive damages where the defendants were accused of misappropriating trade secrets that included algorithms and computer codes. CI professionals can avoid becoming part of these embarrassing and possibly career ending situations by using good judgment and strictly following the Society of Competitive Intelligence

Professional's (SCIP) ethical guidelines. Discretion remains the better part of valor: exercise caution, don't take unnecessary risks.

SCIP's paramount goal is to promote competitive intelligence as a discipline bound by a strict code of ethics and practiced by trained professionals. Properly conducted CI is not espionage and is not spying. Espionage and spying consist of the use of illegal means to gather information. In fact, economic espionage and spying represent failures of CI. SCIP's Code of Ethics is listed at www.scip.org under the "About" tab. CI professionals should continually refresh themselves on these guidelines.

BEST PRACTICES CI OFFENSE

A CI professional should gather intelligence by examining published information sources, conducting interviews, and using other ethical information gathering methods. A skilled CI professional can by deduction and inference fill gaps in information already legally gathered. Some of the best practices for gathering intelligence in an ethical manner are listed in Sidebar 1.

BEST PRACTICES CI DEFENSE

Advances in technology and telecommunications have increased the issues companies face in keeping their trade secrets adequately protected. The widespread use of laptops, personal digital assistants, cell phones, iPhones, wireless internet, pocket cameras, portable external hard drives, miniature flash drives, etc. make it easy for employees, especially disgruntled current and former employees, to misappropriate confidential information.

Employee mobility and company assets in the form of digital information, combined with fast and easy methods for transferring data, has increased the need for creative trade secret protections. A company's most valuable secrets can be compromised with the simple touch of a screen. Additionally, the increasing popularity of social networks and online forums, such as such as Facebook®, MySpace®, LinkedIn®, and Twitter®, provide numerous opportunities for employees to intentionally or recklessly leak proprietary information. Sidebar 2 lists some of the best practices for sealing leaks.

ALWAYS KEEP ON THE RIGHT SIDE OF THE LINE

Competitive intelligence is an important aid to a company in the marketplace if it is gathered properly. However, if the information is gathered improperly, the information ceases to constitute competitive intelligence at all, and can result in detrimental and serious consequences for the CI professionals involved and their company.

The line between ethical and unethical may be fine at times and for that reason CI professionals must always keep that line at the forefront of their minds and consult legal counsel in those grey areas. CI professionals can also add tremendous value by assisting their companies to effectively protect their valuable information against disclosure. An effective and conscientious CI professional should always seek to abide by SCIP's Code of Ethics and should strive to utilize the best practices outlined above for successful CI Offense and CI Defense.

Michael D. Wexler is a partner in the Seyfarth Shaw LLP Chicago office and is national chair of the firm's Trade Secrets, Non-Competes, and Computer Fraud group. A former state prosecutor, he focuses on trial work and counseling in the areas of trade secrets and restrictive covenants, corporate espionage, and intellectual property infringement in both federal and state courts. Michael has a BA from the University of Illinois and a JD from IIT Chicago Kent College of Law. He can be reached at mwexler@seyfarth.com.

Robert Milligan is a partner in the Seyfarth Shaw LLP Los Angeles office, and has extensive trial and pretrial experiences in a variety of commercial litigation matters, including trade secrets, Sarbanes-Oxley Act proceedings, and unfair competition litigation. He has conducted numerous trade secret audits and is an accomplished speaker and lecturer in the area of trade secrets. He has a BA from Gonzaga University and a JD from University of California, Davis. Robert can be reached at rmilligan@seyfarth.com.

A special thanks to Seyfarth Shaw LLP summer associate Alana Friedman for her assistance in helping Michael and Robert prepare this article. Both Michael and Robert are regular contributors to the Firm's law blog on Trade Secrets, Non-Competes, and Computer Fraud, www.tradesecretslaw.com.