30-SECOND SUMMARY

When an integral employee decides to leave, clients must be maintained, coverage ensured and investor relations handled. Most importantly, confidential company information must be secured. Non-compete agreements are no longer enough to deal with the departure of a key employee. A few best practices for protecting your business's electronically-stored secrets include: identifying what types of information are confidential, developing a trade secret protection policy, implementing security safeguards, conducting compliance training and establishing an exit protocol for employees.

WHEN THE NON-COMPETE IS INCOMPLETE:

Avoiding Trade Secret Litigation

By Vernon Byrd and Larry Turner

Your company's marketing and strategic planning officer for the company's best-selling product, Ms. Smith, announces to her boss and team that she is leaving the company. She tells them that she is joining a competitor. She states, however, that her new duties and responsibilities will not overlap with her duties for your company. Your company's human resources (HR) representative is concerned, but takes her through the company's exit process, which does not include a review of her company laptop. Her laptop is given to the company's information technology (IT) support group, "processed," and issued to another employee. Weeks later, HR and various business leaders reach out to you because they are very concerned about Ms. Smith's new position and the information she may share with the competitor. Little do they know that Ms. Smith's son-in-law is a computer expert who helped her to download more than 50,000 documents — including your company's strategic plan for the next five years, chemical formulas for the products on which she worked and the strategic plans for other products. When this comes to light during the subsequent investigation, Ms. Smith initially responds that she just downloaded a few personal pictures and benefits documents. Her son-in-law and his role are discovered much later.

Keep your eyes on the prize when a key employee departs

Don't add insult to injury

When a key employee announces that she is leaving, it can wreak havoc on the business side. Maintaining clients, ensuring coverage and managing investor relations — all of these things come into play. But the inconvenience of an employee departure can turn into a serious problem requiring an enormous outlay of resources if misappropriation of confidential information becomes an issue. Simply having non-compete agreements with key employees is no longer enough. To avoid having a bad situation turn worse, there are a few steps to take immediately when a key employee departs, as well as day-to-day best practices that should be integrated into your business and its policies.

Day-to-day best practices

1. Know what's in the vault

The first thing that corporate counsel must do to protect against disclosure of confidential information is to clearly identify what types of information are confidential or proprietary. A vague or ambiguous policy will not do; only where it is clear that certain information is to be treated as confidential will protections be sufficient. Similarly, not everything can be confidential. The protection loses its teeth when YouTube videos or take-out menus are designated as "confidential." While it may require some resources to ensure that confidential information is designated and maintained appropriately, it is a wise investment to protect that information.

It also is important to identify who has access to the various types of confidential information so that you know who the key players really are. The day an employee leaves the company is not the time to learn that she could have taken your secrets with her.

2. Develop a detailed policy

There is no such thing as an effective one-size-fits-all confidentiality/trade secret protection policy. Each company has unique assets and resources, requirements and restrictions. If your company does not already have a policy regarding intellectual property (IP), work product, confidential information or trade secret protection, it is vital that you develop such a policy. In the event that an employee subverts the policy on confidential information and provides trade secrets to a new employer, that well-defined and strictly managed policy can make all the difference in enforcing a later action for misappropriation. The employer will be required to demonstrate that it took appropriate steps to protect its confidential information, including enforcing policy protocols.

At a minimum, a sound policy on confidential information should include:

- the company's expectations for its employees regarding confidential information, including a prohibition on unauthorized copying or disclosure;
- a definition of what is considered confidential or proprietary, including as many specific types of information as possible;
- the consequences to the employee for violations of the policy, and the rights of the employer in the event of a violation;
- the employee's responsibility to return all company technology and confidential information before leaving employment;
- a mechanism for ensuring that employees receive the policy and sign an acknowledgment of their responsibilities under the policy; and
- continuous training of key employees on a regular basis as part of the company's compliance program.

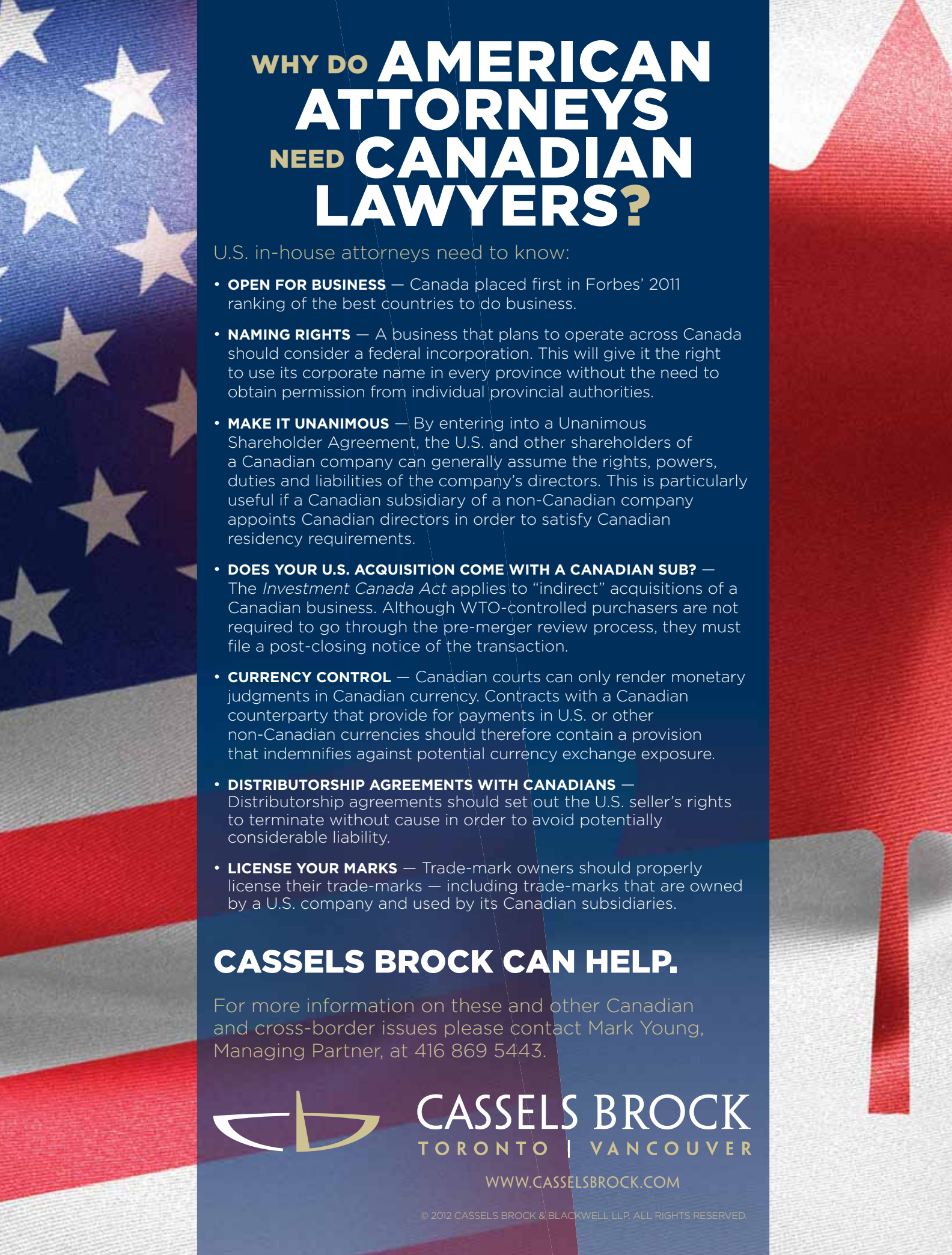
3. Establish security protocols

A well-drafted and publicized policy will do little if it is not enforced with certain day-to-day security safeguards. Appropriate security measures must include limits on access to confidential information of all forms. Locks on file cabinets do nothing to secure ESI in the digital world. For example, password requirements for accessing or sharing certain types of information are now widely employed. Understand how to limit access to databases and other information repositories, and make sure your systems can track who can access, modify or delete information. This is important not only for protection, but also for enforcement. For example, to succeed in a civil action against a former employee for violation of the Computer Fraud and Abuse Act (CFAA)[1] or the Stored Communications Act (SCA),[2] an employer must demonstrate that the

Vernon Byrd is executive director, Center for Legal and Credo Awareness, and assistant general counsel for Johnson & Johnson. As assistant general counsel, Byrd is a member of the Johnson & Johnson litigation group with a specialty in employment litigation. *vbyrd1@its.jnj.com*

Larry L. Turner is a partner in Morgan Lewis's Labor and Employment Practice and co-chair of the firm's Diversity Committee. He is resident in the firm's Philadelphia office. *lturner@morganlewis.com*

The authors would like to thank Michael C. Higgins and Margit E. Anderson, associates with Morgan Lewis & Bockius LLP, who also had substantial input in this article.



WHY DO AMERICAN ATTORNEYS NEED CANADIAN LAWYERS?

U.S. in-house attorneys need to know:

- **OPEN FOR BUSINESS** — Canada placed first in Forbes' 2011 ranking of the best countries to do business.
- **NAMING RIGHTS** — A business that plans to operate across Canada should consider a federal incorporation. This will give it the right to use its corporate name in every province without the need to obtain permission from individual provincial authorities.
- **MAKE IT UNANIMOUS** — By entering into a Unanimous Shareholder Agreement, the U.S. and other shareholders of a Canadian company can generally assume the rights, powers, duties and liabilities of the company's directors. This is particularly useful if a Canadian subsidiary of a non-Canadian company appoints Canadian directors in order to satisfy Canadian residency requirements.
- **DOES YOUR U.S. ACQUISITION COME WITH A CANADIAN SUB?** — The *Investment Canada Act* applies to "indirect" acquisitions of a Canadian business. Although WTO-controlled purchasers are not required to go through the pre-merger review process, they must file a post-closing notice of the transaction.
- **CURRENCY CONTROL** — Canadian courts can only render monetary judgments in Canadian currency. Contracts with a Canadian counterparty that provide for payments in U.S. or other non-Canadian currencies should therefore contain a provision that indemnifies against potential currency exchange exposure.
- **DISTRIBUTORSHIP AGREEMENTS WITH CANADIANS** — Distributorship agreements should set out the U.S. seller's rights to terminate without cause in order to avoid potentially considerable liability.
- **LICENSE YOUR MARKS** — Trade-mark owners should properly license their trade-marks — including trade-marks that are owned by a U.S. company and used by its Canadian subsidiaries.

CASSELS BROCK CAN HELP.

For more information on these and other Canadian and cross-border issues please contact Mark Young, Managing Partner, at 416 869 5443.

CASSELS BROCK
TORONTO | VANCOUVER

WWW.CASSELSBROCK.COM

employee exceeded his authorization to the electronic information at issue.[3] Having clear protocols in place may make it easier to show that certain access was unauthorized and exceeded the employee's authority. A skilled IT department manager or outside consultant will be able to assist in identifying appropriate security practices.

Another protection tool is to embed identifiers or tags for especially confidential or sensitive information that can appear on any electronic or printed copy. This would make clear to anyone in possession of the material that the information is confidential and proprietary property of the company.

Additionally, counsel must understand the company's ESI storage and destruction policies. In addition to concerns about unintentional spoliation of evidence based on automatic deletion or overwrites, be mindful of how data or information could be intentionally destroyed. For example, ensure that employees are not able to download software that can "wipe" or overwrite memory to their company-owned laptops.[4] Understand what your company's ability is to investigate whether data has been deleted, copied, removed or transmitted. In the event of a security breach, immediate action may be needed — you should not be just getting up to speed on what your internal systems can do. Understand the resources available to you within your organization so that you will quickly know when it is appropriate to recommend the retention of a forensic investigation or retrieval expert.

4. Enforce compliance

Even if your company has robust confidentiality and security policies, they mean nothing if they are not followed. IT departments can perform certain reviews relatively easily and regularly. However, it is also wise to consider a more robust periodic audit, including an occasional forensic audit to determine to what extent any policies are being violated or are otherwise ineffective.

Think about ways to communicate the message that will be effective for your organization, but also persuasive to a judge if you have to defend your company's process later.

Similarly, periodic reminders of the policy and what information is considered confidential or proprietary are important. In-person training sessions or online webinars can be effective and also allow an employer to ensure that each employee has participated. Simply handing a copy of the policy to a new employee isn't enough. In the event of litigation, the company must have a compelling story to tell about the proactive steps it has taken to protect its confidential information. Think about ways to communicate the message that will be effective for your organization, but also persuasive to a judge if you have to defend your company's process later.

It is also important that protective practices are enforced for all levels of the company. Consistent application of IP and confidentiality policies will act as a deterrent, and will also help in the event of litigation to show that the company has taken reasonable steps to secure confidential information. While all of these steps may require a financial investment, proactive attention to these issues can protect the company's most valuable assets, and make it easier to enforce confidentiality agreements down the line.

Take immediate steps with key departing employees

Now that you've gotten the house in order, what do you do once you learn that a key employee is leaving? How do you ensure no vital information walks out the door? For example, what if your key employee transfers photographs of her kids stored on her work computer to a portable flash drive, but "inadvertently" also copies thousands of confidential files? It is entirely possible that an employee may have confidential information and not even know it. You must take steps to ensure that your company's proprietary information stays safe.

Having a well-established exit protocol for key employees will help prepare everyone for the transition. Here is a list of steps to consider as part of such a protocol:

- Establish an exit interview team that is familiar with the employee's work, projects and external relationships (Exit Team).
- The Exit Team should include the HR personnel responsible for the employee, the business head to which the departing employee reports and does work, and an IT representative, as well as a member of the company's legal department and company personnel familiar with the employee's outside business relationships and connections.
- The Exit Team will develop questions and specific protocols for the departing employee's exit process. Counsel should review the questions and protocols.
- Immediately restrict access to certain files and set a date-certain for the departing employee's return of computer equipment, mobile devices and security badges.
- Consider engaging IT or security department personnel in an analysis of whether the employee copied, transmitted or destroyed key information prior to the submission of his resignation notice.
- Provide a written copy of the confidential information policy to the employee and name individuals whom the employee

WHAT WE OFFER IN RETAIL IS SPECIAL.
HENCE, THE COUPON.

VORYS

Higher standards make better lawyers.®

For more information on our work in retail, visit vorys.com/retail.

SPECIAL RETAIL OFFER!

At Vorys, we've helped some of the largest retailers in the country with their toughest, most complicated challenges - and we can do it for you. From data security issues to labor and employment issues; from M&A and licensing and promotions, to intellectual property, and real estate, and tax issues and more - our attorneys bring decades of experience to every conceivable retail scenario. For more information, visit vorys.com/retail. **ACT NOW!**

Vorys, Sater, Seymour and Pease LLP 52 East Gay Street Columbus, Ohio 43215

Columbus Washington Cleveland Cincinnati Akron Houston

Pre-exit interview questions

Briefing employees on confidentiality expectations before they depart can prevent problems down the road. Do not wait until the employee's last day; talk with your employee as soon as possible, once you know that person is leaving. Below are some questions or points to consider including in your pre-exit interview:

- **Do you have any company or proprietary information in files at home?**
- **Have you used your home computer for company work?**
- **Do you use your personal mobile device (smartphone or tablet) for work?**
- **Have you used a flash/USB drive or cloud for work purposes?**
- **Have you downloaded or otherwise transmitted documents to any of your personal accounts? If so, why?**
- **Does anyone else have access to your electronic work files and accounts?**
- **Do you understand that you must work with the IT department to return all company information from any source, including your home accounts? This also includes retrieving personal information from company systems; we'll help you do this properly so that you do not inadvertently violate the policy.Do not copy, alter, download or delete files without conferring with the IT department. You may violate your obligations as an employee if you do so.**
- **Have you upheld the confidentiality policy and do you agree to continue to do so?**
- **Has anyone asked you to violate the policy or to otherwise obtain confidential information for that person's benefit? Remember that if you are solicited to provide confidential information to anyone, your duty as an employee is to inform the company immediately.**

Best practices such as these will help your company protect against disclosure of confidential information, as well as prevent litigation headaches down the road. Remember that the best prevention is a clear message regarding your policy, repeated often and enforced consistently.

can contact to go over any questions about the policy.

- Schedule a pre-departure interview to remind the employee of the confidentiality policies and review the company's expectations with respect to confidential information and ESI. Representatives from human resources and information technology/security should be present. [SEE SIDEBAR]
- Ask the employee if any company confidential information is on the employee's personal computer.
- During the interview, give explicit instructions not to copy, send, download or transmit information of any kind outside of the company; ask the employee to sign an acknowledgement of receipt of both the policy and the request not to transmit information.
- Follow up the interview with a letter reminding the employee of these responsibilities. Ensure that this letter is given to all employees prior to departure.
- Request that the employee work with the IT department to retrieve any personal, non-confidential information from company computers and explicitly instruct the employee not to download, email or transmit materials without explicit permission and assistance from IT. Even if the employee only wants to download photos of his kids or similar files from his computer, make sure he understands that he should not perform any copying, modifying or destruction of files without getting IT involved.
- On the employee's last day, ask him to again sign an acknowledgement that he has followed the applicable protocols.
- Consider sending a letter to the new employer describing the steps your company took to protect its confidential information and your former employee's obligations with respect to confidential information.

Avoiding a Trojan horse: Best practices when hiring key employees

The honeymoon is over

Your company is thrilled to have wooed a key employee who can add value. Even if you've determined that there are no non-compete issues, your job does not end there. A new employee who brings confidential/proprietary information from his former employer can expose your company to liability, even if no one at your organization asked him to, and even if the transmission is wholly unintentional. You must take proactive steps during the hiring process to ensure that confidential or proprietary information from a competitor does not end up in your company's possession, exposing it to serious expense and liability.

For example, in a recent Utah case, a default judgment was entered against the defendant company in a misappropriation of trade secrets matter after it was discovered not only that employees who had left their employment with the plaintiff to join the defendant had brought over the plaintiff's confidential information, but also that the defendant's executives had destroyed those files despite litigation hold protocols, and then lied under oath about the destruction.[5] While this nightmare for counsel might be an extreme example, all companies must take proactive steps to ensure that new

employees do not bring along a Trojan horse of competitor information that would expose them to liability.

This threat isn't just one where the specter of damages looms if a case for misappropriation is made or where an injunction could be issued; real expenses may be incurred before the employee even starts his employment. When a company must search its information management systems to prove that no confidential information has been brought over by a new employee, it can easily cost tens of thousands of dollars.

Protective policies

Again, having explicit company policies in place — here, prohibiting the solicitation or dissemination of other companies' confidential or proprietary information — may help save the day. Including language within the confidential information policy regarding employees' legal and ethical obligations with respect to competitors' information will demonstrate that the company is not interested in acquiring secret information through unauthorized means.

Similarly, it must become standard practice to make incoming employees aware of this policy. Waiting until an employee starts working may be too late. Even given the sensitive nature of employment negotiations, it is important to clearly communicate that the company is not interested in acquiring the confidential information of the potential employee's current employer. Sending a discreet letter to this effect during final negotiations is one step that can demonstrate the company's good-faith efforts to prevent acquiring competitors' information. The letter should include a reminder for the employee to work with his current IT department to gather any personal information, and to confirm that any information he takes with him is approved by the employer.

If the incoming employee will be subject to an employment agreement, consider including a clause in the incoming employee's agreement making a violation of the policy grounds for termination of the agreement by the employer. An indemnification clause protecting the employer from gross violations of the policy may also be considered, although its enforceability may depend on the circumstances surrounding any violation.

Awareness and training

It is also important that the new employee is reminded of this portion of the confidential information policy during the orientation and training process. Consider having representatives from the legal and IT departments meet with the employee to explain and reiterate the policy, and to obtain an acknowledgement of the policy from the employee.

Additional preventive measures may be worth considering. Confer with your IT department to develop a protocol for discovery and quarantine in the event that the company becomes aware of a possible issue with a competitor's confidential data. Having a well-planned protocol in place will save valuable time. Further, ensure that as part of your IT department's regular review of the efficacy of its confidential information protections, IT is ensuring that competitors' information has not found its way into the system. Also, creating a means for employees to report possible violations of the policies underscores the seriousness of the policies. Make sure that employees know whom they can contact in the event that they believe there may have been a violation. Heading off these issues at the pass can limit an employer's vicarious exposure to liability.

Documentation

Documentation of the company's efforts to ensure that it has not improperly acquired others' confidential information is crucial. Trainings must be well documented with records of attendees and with written copies of relevant policies provided to participants. Documentation of all efforts to prevent incoming employees from transmitting confidential data must also be created contemporaneously. Self-serving deposition testimony after the fact that "we told him not to do that" will rarely be compelling. Similarly, merely having a policy will be ineffective if new employees are not made aware of it in a timely manner, and if current employees are not reminded of their continued obligations not to solicit or acquire competitors' confidential information and to report possible violations of the policy.

Dispute strategy: Duties for maintaining and preserving electronic data when problems arise

What you need to know

Sometimes, of course, even the best prevention strategy isn't enough. What happens if you discover that a former employee has copied sensitive files, or if you are served with a cease and desist letter from a competitor after a new hire comes on board? Counsel must take immediate action to preserve relevant information in the event of litigation concerning confidential or trade secret information. But what do those duties entail, and when do they arise? It might be more complicated than you think.

As soon as the company is aware of possible litigation, an effective litigation hold must be issued. Simply telling employees not to destroy files will not be enough. As with any litigation, a hold must be descriptive of the information necessary to retain and must be distributed to the appropriate individuals. As the potential issue evolves, make sure to revisit the litigation hold often and update it as new information becomes available. Redistribute the hold periodically to remind employees of their continued duties.

Similarly, determine what preservation steps can be reasonably taken with your IT department to preserve server information, backup tapes or other company data. In most instances, an individual's computer or email account will be implicated, so consider taking images of hard drives or mobile devices as soon as possible. As a practical matter, you need to confer with the IT department to determine what sort of notice will be provided to employees that their hard drives or other devices will be searched. If you believe there may be any chance that an employee could attempt to deliberately destroy data, take steps to understand what, if any, intentional destruction could actually be effected by the employee, as well as ways you can prevent it. All of these steps should be well documented by in-house and outside counsel as part of the litigation preparation process, and counsel must take steps to protect the work-product privilege.

Consider whether it may be advantageous to send a letter to the other side, reiterating your company's efforts to protect confidential information and that the company has taken steps to prevent competitors' information from being obtained by its employees or potential employees. Also, consider whether to offer to cooperate with the competitor to identify any potentially confidential information in your possession and to quarantine such information if discovered. Cooperation at the beginning may prevent escalation of the issues, but also may be futile if the other side is determined to engage in litigation.

While the process of disseminating litigation holds and preserving information at the first inclination of potential litigation is not without expense and effort, early preservation efforts may prevent the company from being taxed with fees or costs based on spoliation issues later.

Obligations to preserve

Although the need to preserve information is obvious, it isn't always clear when that duty actually arises and what types of information must be preserved. Unfortunately, there is no one-size-fits-all answer to the question of what must be preserved, as it will depend heavily on the factual circumstances of the case and the type of information that was allegedly misappropriated. The good news is that preservation efforts do not have to be herculean to be effective; rather, they must be reasonable and proportional.

Courts have provided some guidance on when the duty to preserve arises in different situations. For example, in a case involving an employee who had left his former employer to work for a competitor, the former employer's duty to preserve information that could have provided possible defenses to a misappropriation claim was triggered when the employer reasonably anticipated litigation. However, the former employer did not engage in spoliation where, at the time it anticipated litigation, it was not aware that others in the organization had possibly gained the competitor's information, and therefore, the employer was not responsible for preserving all files for those individuals at that time.[6] In that case, the duty to preserve information for those individuals came once the former employer learned that they might have relevant files, but by that time, some had been destroyed. The fact that files were not preserved was not sufficient to warrant spoliation sanctions. Importantly, the former employer's demonstrated policy against misappropriation of information, and its reminders to employees of their legal and ethical obligations with respect to competitive intelligence, also swayed

Additional resources

Corporate Compliance Series: Designing an Effective Intellectual Property Compliance Program (Sternstein, Kaplan, Frankel, Dolan) (2011).

ACC EXTRAS ON… Workplace information and non-competes

ACC Docket
Non-compete Agreements in the United Sates, Europe and Australia (April 2011). *www.acc.com/docket/nca-us-eur-aus_apr11*

InfoPAK℠
Workplace Information Risk in the Digital Age: Monitoring Employees, Social Media Challenges, Managing Access to Data and Optimizing Flexibility (Jan. 2011). *www.acc.com/infopaks/info-risk_jan11*

Top Ten
Top Ten Considerations for Non-compete Clauses in Europe (The Netherlands, Belgium, Spain, Germany, France, Italy) (June 2011). *www.acc.com/topten/non-compete-eur_jun11*

Form & Policy
Sample Confidentiality and Non-compete Provisions Executive Employment Contract (May 2009). *www.acc.com/forms/non-cmpt_may09*

Presentations
Drafting Non-competes: Five Things To Do Before Picking Up the Pen and Five Things to Think About After You Do (Oct. 2011). *www.acc.com/draft-non-cmpt_oct11*

Protection of IP with a Focus on Trade Secrets for the Non-specialist (Oct. 2011). *www.acc.com/protect-ip_oct11*

Article
Non-Compete Clauses: An International Guide (Jan. 2011). *www.acc.com/ncc-intl_jan11*

ACC HAS MORE MATERIAL ON THIS SUBJECT ON OUR WEBSITE. VISIT *WWW.ACC.COM*, WHERE YOU CAN BROWSE OUR RESOURCES BY PRACTICE AREA OR SEARCH BY KEYWORD.

Offices in
Beijing
Brussels
Century City
Chicago
Del Mar Heights
London
Los Angeles
New York
Orange County
Palo Alto
San Diego
San Francisco
Santa Barbara
Seoul
Shanghai
Washington, DC

Many people believe that law firms are pretty much the same. We don’t. We believe that what separates us from the pack is not what we do, but how we do it. Aggressive not conservative, team players not one-man-bands, problem solvers not just legal practitioners. Our clients clearly understand and value this difference.

How can we help you? Contact our Chairman, Guy Halgren, at 619.338.6605.

SheppardMullin

sheppardmullin.com

Where a departing employee had extensive access to company trade secrets/ confidential information, an independent forensic investigation will be crucial.

the court against an adverse inference that information that was lost was probative of the issues in the case.[7]

On the other hand, when is a potential defendant "on notice" that ESI must be preserved? Courts have found that when an action is filed, a duty to preserve is definitely triggered. For example, in an action alleging improper access to a secure dealer server by a former employee now working for a competitor, the competitor was not required to preserve information before the suit was filed, even though the competitor was aware that its employees may have improperly accessed the server. However, once the suit was filed, the duty to preserve was triggered, and the competitor/ defendant was responsible for ensuring that a timely effort was made to collect and preserve evidence. Because the defendant waited for three months to even confirm that individuals were aware of and abiding by the litigation hold, the court sanctioned the defendant by making it pay for the costs incurred for the forensic examination of the defendants' computers, as well as attorneys' fees incurred by the plaintiff in bringing the motion to prevent spoliation.[8] The court noted that "[i]n order to avoid sanctions, such as these, parties must cooperate and voluntarily preserve, search for and collect ESI."[9]

The forensic examination

In cases such as these, the forensic examination and collection process is paramount. Simply relying on employees to voluntarily disclose information regarding misappropriation is likely to be wholly insufficient. An in-house IT department may be too close to the relevant individuals to conduct a truly independent investigation. Counsel must consider whether an independent forensic examination is best. Where a departing employee had extensive access to company trade secrets/confidential information, an independent forensic investigation will be crucial. It is important to note here that a forensic examination is not the same as a typical document review. A forensic examination deals with examining ESI systems and history, rather than the content of the ESI itself. This is one area where you might consider seeking to share costs with opposing counsel because forensic examinations can be costly. However, it is critical to understand your company's particular situation and systems before making any promises regarding forensic examination. Don't promise what you can't do!

Conducting an independent forensic examination very early on may demonstrate that the company's systems do not contain misappropriated information, and may also help to convince the court that the company takes its confidentiality policies and procedures seriously. Even if issues are discovered, getting them out in the open at the beginning, rather than after prolonged discovery, can make all the difference in how a case progresses.

Have a compelling story

As counsel, you want to be in a position to tell a compelling story to a competitor's counsel, judge or jury, explaining how your company has taken significant efforts to prevent issues relating to misappropriation of information. By clearly defining policies, communicating them effectively and often, and taking a few other commonsense precautions, your company may save itself serious litigation headaches down the road. While the investment on the front end may require some justification, it could be what saves the day in the end. **ACC**

NOTES

1 18 U.S.C. § 1030.
2 18 U.S.C. § 2701.
3 *See Penrose Computer MarketGroup, Inc. v. Camin,* 682 F. Supp. 2d 202, 210-12 (N.D.N.Y. 2010). District court denied a motion to dismiss CFAA and SCA claims based on allegations that employee accessed his boss's email account and obtained proprietary information, but dismissed SCA claims based on allegation that employee deleted his own work email. There is a split between the Circuits regarding the application of CFAA.
4 In a recent Utah case discussed *infra*, employees downloaded software with the ability to "wipe" or permanently delete files from their laptops, in an attempt to conceal their misappropriation of their former employer's confidential information. The IT expert retained by the plaintiff discovered the fraud and was able to show that the file names of the destroyed documents were likely highly relevant to the litigation. As a sanction for these and other transgressions, default judgment was entered against the defendant with an award of attorneys' fees to the plaintiff. *Philips Elec. N. Am. Corp. v. BC Technical*, 773 F. Supp. 2d 1149, 1158-59 (D. Utah 2011).
5 *Philips Elec.*, 773 F. Supp. 2d at 1158-59. The case was also referred to the United States Attorney's Office for investigation of alleged perjury.
6 *E.I. Du Pont de Nemours & Co. v. Kolon Indus., Inc.*, Case No. 3:09cv58, 2011 WL 1597528, at *13-18 (E.D. Va. Apr. 27, 2011) (denying motion for sanctions for spoliation of evidence where court determined that plaintiff had taken reasonable steps to preserve when it became aware of additional possible sources of information).
7 *Id.* at *18.
8 *Nacco Materials Handling Grp., Inc. v. Lilly Co.*, Case No. 11-2415, 2011 WL 5986649 (W.D. Tenn. Nov. 16, 2011).
9 *Id.* at *13.