KEEPING IT CLASSIFIED

HERE'S HOW TO STAY SAFE IN A TECHNOLOGY-DRIVEN WORLD. BY BILL LONG AND JOHN W. SMITH T

Protecting a company's confidential information is becoming more difficult as technology continues to advance. Plus, an increasingly mobile workforce poses increased risk that employees will breach a company's security measures guarding vital data. Enhanced methods for protecting corporate trade secrets are needed. This article outlines best practices for keeping sensitive information safe.

EMPLOYEE AGREEMENTS AND HANDBOOKS

Noncompete and confidentiality agreements remain one of the most effective tools for mitigating trade secret theft by departing employees. They are enforceable in most places, but should be tailored to comply with the law of the relevant jurisdiction. Legal counsel should be consulted. Agreements must describe the legitimate interests that the company is trying to protect, including the specific trade secrets important to the company. Company handbooks should also include policies that stress the importance of safeguarding confidential information. Couple these with computer use policies that allow companies to investigate the employees' electronic devices.

HIRING/TERMINATION PROCEDURES

On the front end, new employees should sign noncompete and confidentiality agreements and receive orientation emphasizing the importance of safeguarding proprietary information. All training should be documented and repeated periodically, and the noncompete and confidentiality agreement reviewed to make sure it remains current with applicable law.

On the back end, conduct exit interviews with departing employees and document that the employee has returned all property, including all company devices, using a check list that has been updated to reflect the devices assigned to the employee. This requires effective practices for tracking all company property provided to the employee during the employment relationship. Remember that company property includes data that may have been transferred to an employee's personal device. It is good practice to provide a formal separation letter to the employee that confirms that the employee is bound by the noncompete and confidentiality agreement and that the employee acknowledges returning all company property.

Immediately review any returned devices, especially if the employee is going to work for a competitor or if the employee worked in a sensitive position. Most companies of significant size have a dedicated IT staff, but IT staff members are

often very busy and unable to devote immediate attention every time an employee departs. Also, corporate IT employees don't often have experience with the specialized forensic skills needed to detect electronic trade secret theft, including properly preserving electronic evidence for use in litigation against a former employee or a competitor. Bear in mind that the individuals conducting the forensics investigation will often be important witnesses in lawsuits involving trade secret theft. For this reason, it may be prudent to designate and train certain members of the IT team or retain outside consultants who specialize in electronic forensics investigations.

INTERNAL STEPS TO PROTECT CONFIDENTIAL INFORMATION

It is important to demonstrate a robust internal system for protecting trade secrets and other confidential information if a company takes a departed employee to court. On top of having comprehensive policies referenced above, key elements of such a system include:

- ❑ Identifying specific confidential information, noting why it is important, and keeping the list current;
- ❑ Storing the information safely, using the right technology; and
- ❑ Training all managers to mark and safeguard confidential work product.

DATA SECURITY

It is important to know which employees have access to digitally stored information. Requiring pre-approval before an employee is granted access is a good first step, but requests and approvals must be documented. Consider giving read-only access and making the access temporary. Segregate digital information so that access is confined to discrete categories. This prevents "fishing expeditions" by employees.

Companies should review their log-on procedures and use electronic notifications that reiterate confidentiality policies. These notifications help rebut an employee's contentions that he was not aware that the information he downloaded belonged to the company. Other tools can monitor not only access but also user patterns and other computer activity that would indicate unauthorized access, or the downloading or deletion of files. Again, consider seeking a computer consultant's advice.

There is always a balance to be struck between guarding against theft and impairing the company culture.

Require employees to use company-issued flash drives that are traceable. In one recent matter, an employee who resigned to work for a competitor ultimately returned over 30 company-issued flash drives that he had acquired during his extended employment period. Although it is relatively simple to ascertain when a flash drive has been plugged into a computer, it is more challenging to determine whether a flash drive that has been returned is the same one that the employee plugged into his computer shortly before resigning.

EMPLOYEE DEVICES

To increase productivity, employees are often encouraged to send documents to their personal devices that enable work off-site. Consider using corporate policies that minimize the employee's expectation of privacy as to occupational usage of personal devices, including provisions giving the company the right to examine and eliminate company materials stored on personal devices.

For company-owned devices provided to employees, such as laptops, ensure that encryption and other safeguards are in place to protect the information in the event the device is lost. Consider limiting the storage capacity on these devices to prevent downloading massive amounts of information. Employees should also be required to periodically exchange devices so that the devices can be reviewed and wiped. This also serves as a reminder that the devices belong to the company and are monitored.

THIRD-PARTY CONTROLS

Finally, carefully monitor information disclosed by employees in meetings with customers and vendors and remind them that disclosure can forfeit the information's confidential status. Document that the information shared with third parties is not to be disclosed further and use non-disclosure agreements as appropriate.

There is always a balance to be struck between guarding against trade secret theft and impairing the culture that makes the company successful. No single method is fullproof; rather, it is crucial to utilize a variety of techniques that both mitigates the risk of theft and enables recognition and recovery in the event a departing employee crosses the line. ❑

Bill Long is a principal with Integrid Inc. and is a digital forensics certified practitioner, a certified computer examiner, a certified fraud examiner and holds the DataRecovery Expert Certification.
John W. Smith T is a partner with Bradley Arant Boult Cummings LLP and a member of the firm's litigation and intellectual property practice groups.