EMPLOYEE TRADE SECRET THEFT
THE THREAT FROM WITHIN

COVINGTON
COVINGTON & BURLING LLP

The Threat from Within:
Theft of Business Critical Information by Company Insiders

by Chris Bracebridge, Kurt Calia, David Fagan, Marialuisa Gallozzi, Robert Haney, Robert Newman, Grace Ristuccia, Richard Shea, Lindsey Tonsager of Covington & Burling LLP

Theft of trade secrets and other business critical information by employees and other insiders is increasing at alarming rates—costing businesses billions of dollars annually. In one recent case, DuPont was awarded nearly $1 billion in damages after a former DuPont employee was found to have shared confidential information with a competitor. The theft was obviously a problem for DuPont, but the damages award quickly became a serious problem for the competitor as well. And the former DuPont employee ended up in federal prison.

Protecting business critical information is not simple. It involves identifying which information is critical, designating that information confidential, establishing practices, procedures, and policies to maintain confidentiality, and being prepared to address immediately breaches that occur. Each step implicates several areas of the law, including data security, privacy, intellectual property, white collar crime, employment, employee benefits and executive compensation, corporate and securities, insurance coverage, and crisis management.

Protecting business critical information requires understanding the benefits the law offers and the legal limits on protective activity, often across multiple jurisdictions. Advance planning is critical. Coordinating efforts to protect critical information therefore requires a comprehensive plan, and the responsibility could appropriately be placed on a company's legal department.

A comprehensive plan to protect business critical information includes three, related parts: (1) preventing theft, (2) planning how to respond should a theft occur, and (3) reducing risk of being accused of theft by others (*e.g.*, through an insider who brings to the company business critical information from a competitor or former employer).

PREVENTING BREACHES

Establish practices to keep business critical information confidential: In general, business critical information is protected only if it is treated as confidential. For example, under the Uniform Trade Secrets Act, widely adopted in the U.S., information qualifies as a trade secret if, among other requirements, "reasonable efforts" are taken to keep the information secret. Whether efforts are reasonable will depend on the type of information and its relative importance to the company. Practices to treat information as confidential include:

> *Limiting access to information:* A company must not only determine which personnel may access information but how information may be used—and stored. A company needs to consider the extent to which employees and other insiders may use personal devices to access and store information. Employees may store confidential information on personal devices, which can be more easily lost or accessible to individuals outside the company. Moreover, a court in New York recently ruled that a company did not have the right to access a former employee's personal iPhone during discovery in employment litigation, even though the employee stored the company's customer information on the iPhone.
>
> *Monitor compliance:* Protecting confidential information could include regularly policing intranet and document management systems and checking outgoing emails for keywords or word combinations related to trade secrets. However, it is important to structure these efforts to comply with local privacy laws.
>
> *Establish and communicate confidentiality policies:* Policies should reflect the importance of confidential information and the breadth of information deserving of protection. Some laws, such as insider trading prohibitions, are well established in company policies, but companies need to confront new ways confidential information may be created, used, and disseminated. For example, business critical information may be carelessly shared in the course of employees' daily posts on social media. Drafting confidentiality policies requires understanding the extent to which companies may limit the use of social media, at work or outside of work.
>
> Establishing robust confidentiality procedures for employees might not be sufficient unless the company requires vendors and other third parties to treat business critical information as confidential. For example, vendor contracts could require third parties to store information on a separate server and not comingle it with information of other clients, who may very well be competitors.

***Incentivize Compliance*:** Adding insult to injury, a company could be required to pay bonuses and incentive awards to a former employee who discloses the company's business critical information. To avoid this result—and encourage compliance—employment agreements and incentive awards can be conditioned on compliance with confidentiality and restrictive covenants, such as covenants not to compete or solicit employees or customers. However, in some cases, broad covenants not to compete or solicit could be invalidated under applicable law. Constructing effective restrictions involves careful analysis of local law. In addition, employment agreements can give a company the ability to protect more information than local

laws by defining "confidential information" more broadly than the law defines trade secrets. Employment agreements are therefore an important source of protection.

***Review insurance coverage*:** The time to consider whether and how to insure against losses from information theft is before an incident occurs. Coverage may be implicated under a variety of policies, including first-party property, third-party liability, cyber-risk, employee dishonesty, crime, and director's and officer's coverage.

RESPONDING TO INCIDENTS

While taking as many precautions as possible, companies should still prepare for the worst. Given the need to act quickly in the event of a possible theft, companies should develop a comprehensive incident response plan, which could include the following steps:

***Decide Whether to Investigate*:** Whether a theft occurred may not be clear initially, and companies must determine whether to investigate. Investigation can be costly and bring unwanted attention to the loss or vulnerability. Investigations can range from forensic computer searches to interviews with employees. A company might need to investigate to determine whether internal controls (which are sometimes imposed by law) are functioning. Many jurisdictions, including the U.K., may require investigation to ensure that subsequent employment action is procedurally fair and legally compliant. A plan of action should address how to decide whether to investigate.

Decide on Employment Action: If a company suspects theft by a current employee, it might consider whether to immediately terminate employment, or wait and investigate. Employment agreements and, particularly outside the United States, employment laws may limit the actions a company may take. Furthermore, a hasty termination may result in losing the ability to collect evidence and verify suspicions. However, immediate action may be required to prevent further loss. A plan of action should include a process to make immediate employment decisions and assess whether to bring in outside counsel and forensic experts to gather evidence quickly.

Decide on Disclosure: An incident response plan should include an approach to determine whether disclosure of a theft (or possible theft) is necessary or desirable—and to whom the theft would be disclosed. Several areas of the law may be implicated, including privacy, securities, and data breach laws. If customer data has been taken, the company might have a legal obligation to notify customers or regulatory agencies (*e.g.*, the U.K. Information Commissioner's Office). Furthermore, the theft might violate criminal laws. For example, in the U.S., the Economic Espionage Act of 1996 makes it a federal crime to attempt to take, or conspire to take, a trade secret. A company might therefore wish to involve federal investigators. Securities laws also might require disclosure for public companies.

Notify Insurers: When there is a loss, companies should notify potentially-implicated insurers immediately and consider retaining coverage counsel and other professionals to assist with navigating the claims process and ensuring that insurers honor policy obligations.

Assess Litigation: Although a costly remedy, companies may determine that civil prosecution is necessary to obtain an injunction or recover damages. Quick action may be required. Trade secret theft may result in civil and criminal proceedings, which will run on separate tracks with separate agendas. A plan of action would include identifying the process for assessing litigation options, including pursuing rights under employment agreements and trade secret laws.

AVOID RECEIPT OF IMPROPERLY TAKEN INFORMATION

A company may be liable if it receives confidential information taken by an individual from another company. A comprehensive plan would include procedures to address this possibility. In 2006, Pepsi received a faxed letter from an individual claiming to be a top-level employee at Coca-Cola offering confidential information to the highest bidder. Pepsi responded by sending this letter to Coca-Cola who involved the FBI. The two individuals behind the scheme now face prison sentences. While Pepsi acted wisely to avoid liability, many incidents of receipt of trade secret theft may be subtler than a letter with an explicit offer. Companies should clearly state in employee policies and handbooks that receipt and use of another company's trade secrets is prohibited. Upon hire, new employees could be asked to acknowledge that they have not and will not bring in any trade secrets from another company. Employees do not always understand what information is confidential. Further probing may be necessary to determine whether the individual has anything at home or in electronic form that might belong to a former employer. Finally, if information of a former employer is uploaded onto the new employer's systems or otherwise shared, careful attention needs to be given to how to remediate the problem, whether and how to inform the prior employer, and how to return the information.