Careless Employees: A Company's Biggest Trade-Secret Threat

By **Audra Dial** (June 19, 2018)

Audra Dial

Careless employees remain the greatest threat to trade secret theft, according to the recently released "Second Annual Study on the Cybersecurity Risk to Knowledge Assets," co-authored by Kilpatrick Townsend & Stockton LLP and the Ponemon Institute. Interestingly, the careless employee plagues companies of all levels of sophistication when it comes to protecting "knowledge assets." This year's survey included a deeper analysis of survey participants who rated their organization's effectiveness in protecting their knowledge assets as very high. Respondents who gave their organization's effectiveness in mitigating the theft of knowledge assets a 9+ ranking on a scale of 1 (not effective) to 10 (highly effective) are identified in the survey as "high performing organizations" and included in the deep-dive analysis. Even among such "high performing organizations," careless employees posed the greatest threat to their knowledge assets, despite greater levels of employee training, audits and restrictions on the access to this high value information at these organizations.

Companies, particularly "high performing organizations," have become much more sophisticated when it comes to training and employee education, according to this year's survey results. Over 70 percent of all survey respondents confirmed that they engage in regular training and awareness programs for their employees to educate them on ways to reduce trade secret theft, and over 60 percent of all survey respondents monitor their employee's actions to ensure that trade secrets are not vulnerable to attack. Of the "high performing organizations," 83 percent engage in regular training and awareness programs, and over 70 percent monitor their employees to identify potential threats to the corporation's knowledge assets. Thus, companies clearly believe that training programs are the most meaningful way to reduce employee carelessness when it comes to protecting corporate assets. However, as the survey results demonstrate, these training programs are not enough to combat the careless insider.

Despite knowing the careless insider presents the greatest threat to corporate crown jewels, the majority of companies responding to the survey do not restrict access to this information to only certain employees. In fact, 52 percent of survey respondents still permit all users, regardless of their status within the organization, to access the company's most important knowledge assets. Given that careless employees are the most likely to put crown jewels at risk and most companies are conducting some form of training for their employees about protection strategies for those knowledge assets, it appears that the leaky pipeline continues to exist, at least in part, because most companies allow all of their employees access to even the most valuable information on the corporate servers.

If companies were to lock down the most valuable electronic information and restrict it to only those individuals within an organization with a specific need to access it, the threat from the careless insider might be greatly reduced. Moreover, removing an employee's access to such information when his job function changes such that he no longer needs to have access to those high value assets is another simple, albeit very effective, strategy for reducing the threats posed by careless insiders.

This conclusion is borne out by the survey results, which show that of the 35 percent of respondents of who rated their organizations as "effective" in protecting their knowledge

assets, 69 percent rated their most effective strategy as restricting access to only those individuals who have a need-to-know specific information. And "high performing organizations" rated their protocols to restrict access to key information to only those employees with a need-to-know that information as one of the important reasons their organizations are most effective in protecting the company's crown jewels. Thus, limiting access to only individuals who need to have access to the company's most important information is a key element in developing layers of protection for corporate crown jewels.

Interestingly, survey respondents identified that the format in which the knowledge assets are kept can be critical in determining how effective a company's protection strategies may be. For example, presentations, product/market information and private communications (particularly in email, texts and social media) containing knowledge assets were identified by survey respondents as the most difficult types of information to protect. In light of this finding, companies would be wise to create policies prohibiting the use of certain formats when disclosing corporate trade secret information. It may behoove companies to institute protocols that forbid employees from discussing trade secret information in written communications, given that email and texts are difficult to monitor and are easy to forward without restriction to others. Moreover, companies should consider whether to have a restricted server to which trade secret information is saved, regardless of format. This procedure could ensure that presentations and communications discussing trade secret information could become more secure than survey respondents currently believe them to be.

Moreover, because companies' crown jewel information remains at risk from careless insiders, companies should consider using trade secret identification audits as a building block for an effective trade secrets protection strategy. Various divisions within a company use and develop trade secret information differently and they store such information in different formats. Thus, employing a cross-functional group to identify and catalog trade secrets can ensure that a company identifies all of its crown jewels. Asking the right questions will help this team to develop an inventory of the company's most valuable information, from which the group can identify the information that should be classified as "trade secrets" and protected accordingly. These questions should include:

- What is the information that the company does not want in the hands of its competitors and is most valuable to the company?
- Who has access to the company's most important information and how is it currently protected?
- In what formats is this information stored?
- Is this information marked and maintained in a restricted manner?

Finally, more than half of the "high performing organizations" conduct assessments of the places most vulnerable to an employee's carelessness or negligence, whereas less than half of the overall survey respondents conduct such audits. Moreover, 65 percent of "high performing organizations" conduct audits to ensure compliance with the policies and protection strategies the company employs for its most important assets, whereas only 54 percent of overall respondents said their organizations conduct such assessments. Utilizing audits that identify key corporate assets, evaluate the vulnerability of those assets to attack and assess employee compliance with policies designed to protect those assets will help companies protect their crown jewels and reduce the risks associated with careless insiders who put corporate knowledge assets most at risk.

As the survey results indicate, most organizations have begun employing more effective techniques to protect their trade secrets from attack. Yet, careless insiders remain the biggest threat to knowledge assets. Thus, companies should step up their protection strategies and add even more lines of defense to their arsenal to reduce these threats and protect their crown jewels from misuse.

Audra A. Dial is a partner at Kilpatrick Townsend & Stockton LLP and managing partner for the firm's Atlanta office.