Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

You Need To Work Harder To Fight Trade Secret Theft

Law360, New York (August 07, 2013, 12:38 PM ET) -- In today's increasingly digital and mobile world, companies are learning — sometimes the hard way — how vulnerable they are to the maliciously inclined employee bent on stealing trade secrets. When Dejan Karabasevic, a top engineer at American Superconductor Corp. (AMSC) used his laptop and the Internet to steal and sell his company's proprietary software to Sinovel Wind Group Co., a Chinese company that was AMSC's biggest client, he nearly destroyed his employer. AMSC's stock plunged, its $1.6 billion market value shrank to $200 million, and 500 employees (more than half the company's employees) were laid off.

On June 27, 2013, a federal grand jury in Madison, Wis., indicted Sinovel, two of its executives, and Karabasevic on charges of conspiracy, wire fraud, and the theft of trade secrets. While the case is still far from over, it is a good reminder of how much work many companies still need to do to protect their most valuable trade secrets from rogue employees with easy access to sensitive information.

In a recent study conducted by Windows privilege management company Avecto, 41 percent of those surveyed identified "rogue employees" as the biggest threat to their organizations. In another study, the network security firm AlgoSec reported that, "insider damage dwarfs outside threats," with two-thirds of respondents rating insider threats as the greatest security risk that organizations face. In its 2012 Confidential Documents at Risk Study, the Ponemon Institute reported that 90 percent of represented organizations had experienced leakage or loss of confidential or sensitive documents in the 12 months prior to the study's completion. In 19 percent of instances, such documents were leaked intentionally by insiders.

Despite evolving security technology and growing awareness, the theft of trade secret information by an employee is still prevalent in part because, unlike a tangible item, an electronically stored trade secret can be stolen with little more than the click of mouse, particularly if an employee already has access to trade secret information. An employee intent on stealing trade secret information may send it using a Web-based personal email account, download it to a personal USB drive, or upload it to a community or public cloud, all without alerting his or her employer.

Organizations are particularly vulnerable to the threat posed by employee use of mobile devices. The Ponemon Institute's 2013 State of the Endpoint reported that 80 percent of those surveyed identified mobile data-bearing devices, such as laptops and smartphones, as posing the greatest security risk to organizational networks. This represents nearly an eightfold increase from just three years ago. Such devices can be used to copy trade secrets or other confidential information from an organization for illegal purposes. And the use of such technology is only increasing in companies. For example, roughly half of respondents reported that the majority of employees in their organizations now use personal

mobile devices in the workplace as bring-your-own-device programs are becoming more common.

Use of third-party applications such as Google Docs and Adobe, and cloud computing infrastructures such as Dropbox, create additional opportunities for determined employees to disclose or send trade secret information outside of the organization. Nearly 70 percent of those surveyed by the Ponemon Institute identified third-party applications as one of the greatest threats to IT security, a 50 percent increase from 2010. Risks caused by removable media and cloud computing infrastructures also rose sharply in the last three years.

Despite recognizing both the threat and the security weaknesses that make it a reality, companies often fail to take the necessary measures to protect against the internal theft or disclosure of confidential information and trade secrets. Even as the threat grows — as computer systems evolve and insider threats become more sophisticated — the threat posed by devices or applications (i.e., a USB device) that can easily be used in a company's own network system (endpoint risk) is not improving. Due to this lack of adequate security, companies often do not know what and how much trade secret information exists outside of the organization's network and if that information is adequately safeguarded.

Common Weaknesses in the Fight Against the Insider Threat

Insufficient Resources

Sixty-seven percent of respondents in the Ponemon study reported that they did not have sufficient resources to counter endpoint risk. Nearly half reported that their IT security budgets would not increase, despite the fact that endpoint risk is increasing.

Manual Processes and Lack of Visibility

Sixty percent of those responding to the AlgoSec survey reported that time-consuming, manual processes, a lack of visibility into security policies, and poor change management were the greatest challenges to managing network security.

Failure to Secure Mobile Devices

Roughly two-thirds of those responding to the AlgoSec survey stated that allowing employees to connect their own devices to the corporate network increased the risk of security breaches. A further 55 percent said that it increased network complexity. Close to one third of Ponemon study respondents reported that their organizations do not secure employee-owned mobile devices. This represents an increase from previous years, despite the fact that use of mobile devices is becoming more prevalent.

Failure to Enforce Use of Cloud Computing Infrastructure

Over half of Ponemon study respondents also reported that their organizations do not regulate employees' use of clouds computing infrastructures, or are unsure if an enforcement mechanism exists. Employees determined to steal trade secrets in such organizations can copy data to these platforms and access it from outside of the organization with little trouble.

Failure to Control Access

Most organizations also do not control employees' local administrative access privileges, thus allowing employees access to sensitive and trade secret information. In 2012, 70 percent of Ponemon study respondents noted that employees had "very frequent or frequent" access to sensitive or confidential documents even where not required by those employees' jobs. Thirty percent of Avecto study respondents reported that they have no policy in place for managing administrator access. With unfettered administrator rights, employees can also download unsanctioned applications to an organization's network, applications that may render the system more vulnerable to theft of trade secret and confidential information.

More than three-quarters of Avecto survey respondents reported that they do not know how many such unauthorized applications have been downloaded on the networks. To make matters worse, more than half of Ponemon study respondents reported that their organizations do not currently plan to improve access governance.

Lack of Communication

Only 13 percent of Ponemon survey respondents reported that collaboration between IT operations and IT security to support planning, communications and information sharing is "excellent."

Strategies for Reducing Risk

There a number of ways that companies can protect their trade secret information, including:

- Developing, implementing and enforcing definitive policies governing the use of personally owned devices, third-party applications, and private cloud computing systems;

- Limiting employee access privileges and enforcing any limitations by, for example, maintaining systems in place to alert IT security personnel of attempted breaches;

- Installing solutions that monitor for key words or phrases in all computer traffic intended for nonapproved recipients or locations outside the organization, and delaying such traffic until it can be reviewed by appropriate personnel;

- Limiting the installation of third-party application or devices, including by implementing application white-listing and privilege management software; and

- Enhancing communication and collaboration between IT operations and IT security personnel.

Corporations cannot afford to bury their heads in the sand, ignoring the insider threat to their trade secrets. They must take decisive preventative measures to avoid becoming the next American Superconductor Corp. and another cautionary tale about the costs of employee theft of trade secrets.

--By Michael H. Bunis and Anna Dray-Siegel, Choate Hall & Stewart LLP

Michael Bunis is co-chairman of the intellectual property litigation group at Choate in

Boston. He also serves as co-leader of the trade secret group. Anna Dray-Siegel is an associate in the firm's litigation department in Boston.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.