Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Avoiding The Risk Of Cybersecurity Whistleblowers

Law360, New York (April 27, 2016, 11:46 AM ET) --
The U.S. Department of Justice's investigation into whether Tiversa Holding Corp. provided false information to the Federal Trade Commission about data breaches at companies that declined to purchase its data protection services heated up this month when the FBI raided the corporate headquarters of the Pittsburgh-based firm. In what marks a growing trend, the government's high-profile investigation began with a whistleblower.


Renee Phillips


Shea Leitch


Aravind Swaminathan

Former Tiversa employee turned whistleblower Richard Wallace alleged in a 2015 FTC hearing that Tiversa provided the agency doctored evidence purporting to prove corporate data breaches. Whether Tiversa's version of the story that it acted as a "Good Samaritan" or the government's claim that the company is in fact running a "Hi-Tech Protection Racket" will prevail may not be resolved for quite some time. The case, however, brings into sharp focus the potential impact that cyber whistleblowers can have, and how organizations can mitigate that risk through thoughtful implementation of protocols and processes.

The Tiversa Investigation

Rumors about cybersecurity firm Tiversa's business practices began to swirl in summer 2014 when ousted Tiversa director of special operations turned whistleblower Richard Wallace — who had been granted immunity from prosecution in exchange for his testimony — testified before the House Oversight and Government Reform Committee. In that hearing, Wallace alleged that Tiversa had provided falsified information regarding the cybersecurity practices of other companies to the federal government.

Wallace's allegations did not stop there. The former technical analyst claimed that Tiversa employees were given the task of scouring Internet file-sharing websites in an effort to find information stolen from or leaked by companies. When such information was found, Tiversa would contact the company and offer to remediate the issues. According to Wallace, if the company refused its services, Tiversa would turn the information over to the FTC. According to a report by the House of Representatives Committee on Oversight and Government Reform, information provided by Tiversa "formed the basis for multiple enforcement actions and dozens of warning letters."

Wallace also provided testimony at an FTC administrative hearing regarding allegedly insufficient cybersecurity practices in high-profile FTC enforcement proceedings against LabMD. LabMD and the FTC both admit that information provided by Tiversa to the FTC was used in the agency's enforcement action against LabMD. Ultimately, Wallace's testimony about Tiversa's conduct cast sufficient doubt on the evidence against LabMD that the administrative judge dismissed the FTC's case against LabMD, showing how a single cybersecurity whistleblower could have a major legal impact.[1]

Incentives for Whistleblowers

Although Tiversa's alleged conduct may be an outlier, a company's conduct need not be malicious — or, necessarily, even culpable — to be susceptible to outing by a cyber whistleblower. Even companies that diligently seek to detect and prevent cyberattacks can become subject to regulator scrutiny by virtue of a whistleblower's tip. And there are incredible incentives for whistleblowers. Not only are they potentially motivated to come forward to try and earn immunity from government prosecution (in an egregious case, perhaps), but some regulators are encouraging whistleblowers to come forward with the lure of monetary rewards in the form of bounty programs.

The U.S. Securities and Exchange Commission has established what is perhaps the most advanced and well-known bounty program. The SEC Office of the Whistleblower invites individuals to report securities law violations in exchange for potentially considerable monetary awards. The SEC has also recently entered the cybersecurity regulation fray, establishing the proposition that the agency views certain cybersecurity failures to be securities law violations. Anecdotal reports from whistleblower lawyers and the SEC's Office of the Whistleblower suggest that many whistleblowers are already approaching the SEC, seeking bounties for violations such as failure to adopt adequate internal controls and failure to disclose risks or incidents to shareholders.

What Can be Done?

Companies need not live in fear of the unknown cyber whistleblowers in their midst, and can take steps to mitigate the risks that a whistleblower will go straight to the SEC or similar agency. Implementing robust internal reporting and investigation processes can encourage internal reporting of concerns. For example:

- Ensure there are numerous avenues available to make complaints (including anonymous complaints) and that employees are aware of those avenues. Employees should be able to lodge a complaint via managers, human resources, compliance, legal, a telephone/email hotline, or a website.

- Be sensitive to the potential for real or perceived retaliation against whistleblowers. Involve legal or human resources in any employment decisions involving a potential whistleblower, including performance reviews, before finalizing.

- Resist the urge to identify an anonymous whistleblower; it is very difficult to retaliate against someone whose identity is unknown. Implement a system by which you can follow up with an anonymous whistleblower that safeguards their identity (i.e., Ethics Point or Hushmail).

- Train information technology managers and other managers on the front lines about what could form the basis for cybersecurity whistleblower complaints and how to properly receive and escalate them.

- Review third-party vendor practices (contractors, consultants, auditors, hotline administrators) to ensure they too provide optimal whistleblower procedures. Make clear in company policies that reports from third parties are also accepted by the company.

- Whistleblowers have a heightened sensitivity to whether the investigation is biased, so consider extra precautions to ensure the neutrality of the investigation.
    - If the complaint involves a manager, HR and legal personnel who support the manager should not be involved in the investigation.
    - If the internal audit department is participating in the investigation, make sure that the audit personnel who work for the area of the business under investigation are not participating in the investigation.
    - If the complaint involves a C-level employee, independent outside counsel should be retained by the audit committee of the board of directors, as opposed to company's inside counsel or regular outside counsel conducting the investigation.

Conclusion

With regulators hungry to identify and investigate potential cybersecurity issues, whistleblowers provide a fertile opportunity to get the inside perspective with little to no resource investment. By creating a safe environment in which whistleblowers can report internally, a company can go a long way toward shielding itself from employee-initiated regulatory investigations.

—By Renee Phillips, Shea Leitch and Aravind Swaminathan, Orrick Herrington & Sutcliffe LLP

Renee Phillips is a partner in Orrick's New York office and co-head of the firm's whistleblower task force. Shea Leitch is an attorney in the firm's Washington, D.C., office. Aravind Swaminathan is a partner in the firm's Seattle office and global co-chairman of the firm's cybersecurity and data privacy team.

[1] The FTC is currently appealing the administrative judge's dismissal of the case. See https://www.ftc.gov/system/files/documents/cases/580032_-_labmd_-_complaint_counsels_notice_of_appeal.pdf.