The Rise of the Cybersecurity Whistleblower

The Recorder | 10.01.15

Cybersecurity

The Securities and Exchange Commission has joined the rising tide of cybersecurity regulatory enforcement. As the potential liability for cybersecurity deficiencies continues to mount, and as cybersecurity-related corporate misdeeds increase, how long before we see the next wave of whistleblowers—the cybersecurity whistleblower? Anecdotal evidence strongly suggests that the SEC is currently evaluating cybersecurity whistleblower claims. Indeed, based on a tip from a cybersecurity whistleblower, the Department of Health and Human Services recently brought charges against a hospital for improperly storing electronic protected health information. So, how should a company prepare for a potential cybersecurity whistleblower?

The Hypothetical Cybersecurity Whistleblower

Company A is faced with a data breach. In responding to the breach, Company A evaluates the costs and benefits associated with publicly reporting the breach and, perhaps short-sightedly and potentially in violation of the law, makes the decision not to report the breach. Alternatively, the company makes the decision to publicly report, but intentionally minimizes the size and scope of the breach. Enter the disgruntled IT manager. Prior to the breach, the IT manager had asked for but was denied funds to purchase a shiny new cybersecurity device, and now feels that the lack of that device contributed to the breach. Importantly, the IT manager's memo outlining the need for the device will have put senior people within the company on notice of the inadequate state of its cybersecurity prior to the breach. Once Company A decides to act aggressively in not reporting the breach, the IT manager may have a strong financial or moral incentive to report the company's perceived misdeeds to the SEC.

Qualifying to Be a Cybersecurity Whistleblower

An "eligible whistleblower" under the SEC's Whistleblower Incentive Program is a person who voluntarily provides the SEC with "original information" about a possible violation of the federal securities laws that has occurred, is ongoing or is about to occur. Importantly, the whistleblower need not be an employee of the company to submit information about that company. See Rule 21F-2. The SEC's 2014 Whistleblower Report noted that 20 percent of the whistleblower award recipients to date were contractors, consultants or potential consultants.

Further, there is no blanket requirement that the employee or contractor report to the company first. The employee or contractor may be able to go directly to the SEC to report the company's misdeeds, however, the SEC has created certain incentives for whistleblowers to first report internally, including a potential for a larger award.

Finally, unlike the average employee, compliance employees do have an obligation to report internally first to be eligible for a whistleblower award. Further, the compliance employee must generally wait 120 days between reporting the issue internally and contacting the SEC. The 120-day waiting period gives the company a little extra time to verify alleged wrongdoing and attempt to remedy any identified issues before a whistleblower reports to the SEC.

Preparing for a Potential Cybersecurity Whistleblower

Borne out of the recognition that there is no requirement that a whistleblower report first to the company before reporting to the SEC, the simplest ways for companies to ward off whistleblowers is to incentivize internal reporting and to take the reports seriously once they are received. Companies should educate all cybersecurity employees on the company's internal reporting structure, which should include an anonymous tip line, and provide appropriate and tangible benefits—including monetary incentives—for internal reporting of problematic conduct. These incentives should also extend beyond the company's employees to contractors, consultants and even customers.

In our hypothetical, the IT manager provided a memo on the need for a cybersecurity device. A company faced with such a memo would be well served by fully assessing the need for the new device. As part of the compliance function, companies typically engage outside parties to conduct cybersecurity risk assessment and/or security audits. Company A should make sure that any analyses of particular cybersecurity measures are up to date and do not support the need for additional equipment. Indeed, it may be prudent for Company A to circle back to the IT manager to explain why the company reached the decision it did. Such conduct may show the IT manager that the company is taking those concerns seriously.

Do Not Impede Whistleblowers

Under SEC Rule 21F-17, companies may not take action to impede individuals from communicating with the SEC about possible securities law violations, "including enforcing, or threatening to enforce, a confidentiality agreement ... with respect to such communications."

Pursuant to this rule, companies should be mindful not to take any action to impede the potential cybersecurity whistleblower from communicating with the SEC about a possible securities law violation, and should eliminate language in form confidentiality agreements or severance agreements that could be interpreted as stifling whistleblowers.

In our hypothetical, Company A should be mindful to conduct an internal investigation of the breach in a way that does not run afoul of the SEC whistleblower protections. It should also not attempt to pinpoint any potential whistleblowers, as the mere outing of a whistleblower can be construed as an adverse employment action and expose Company A to a retaliation claim. *Halliburton v. Administrative Review Board*, Case No. 13-60323 (Fifth Circuit, 2014). Further, if Company A does not know who the whistleblower is, it is much more challenging for the whistleblower to argue that perceived retaliation constitutes actionable retaliation. Rather, the investigation should focus not only on the cause of the breach but also any corporate decisions related to cybersecurity that occurred prior to the breach and arguably could have contributed to the likelihood of the breach. For example, Company A's counsel should ask for any documents the company had in advance of the breach potentially reflecting on the breach. That could point counsel to the IT manager's memo among other documents that counsel may not otherwise know about. Unearthing that memo could be extremely important because the SEC may conclude that those within Company A that reviewed it knew in advance that the company's cybersecurity was deficient. The SEC may infer that Company A's decision to not address those issues reflected an intentional decision to put customer data at risk.

The investigation should be conducted with the knowledge that the investigation itself may get reported to the SEC by the whistleblower. For example, if the investigation is merely a whitewash to support the company's decision not to report the breach, the whistleblower may have a front-row seat to the painting party. The investigation needs to be done in a professional manner that seeks the truth, and doesn't stifle contrary views.

Finally, to the extent Company A is inclined to not report the breach or downplay it, due consideration should be given to whether everyone within the group of decisionmakers is on board with that decision, or at least understands the legal basis for the decision.

Maintain Privilege

Internal investigations should also be conducted with an eye toward maintaining privilege and minimizing the risk of waiver. That way, the company maintains control over whether to disclose the investigation process and results, and the extent of that disclosure. Internal investigations conducted at the direction of counsel are generally covered by the attorney-client privilege and work product protection. *United States v. Chen*, 99 F.3d 1495, 1501 (9th Cir. 1996), cert. denied, 520 U.S. 1167 (1997).

Therefore, attorneys, whether in-house or external counsel, should initiate and direct the investigation. Furthermore, any cybersecurity consultants acting as forensic investigators hired by the company to help investigate the breach should be hired and directed by counsel. That way, the privilege umbrella should extend to the work of the investigators and any report that they prepare.

Mark Mermelstein serves as co-chair of Orrick's cybersecurity and data privacy group. Christin Hill is a senior associate in the labor & employment department at Seyfarth Shaw.

Authors

Mark Mermelstein
Partner, White Collar, Investigations, Securities Litigation & Compliance, Internal Investigations

Los Angeles

D +1 213 612 2204
E mmermelstein@orrick.com

Related Areas

- **Cybersecurity & Data Privacy**
- **Litigation & IP**