COMPLIANCE WEEK
THE LEADING INFORMATION SERVICE ON CORPORATE GOVERNANCE, RISK, AND COMPLIANCE

Avoiding Vanguard's Cyber-security Stumble

John Reed Stark | March 22, 2016

Vanguard experienced a disquieting stumble last month, and seems stuck in an ill-fated state of denial.

Vanguard apparently unintentionally sent 71 emails pertaining to different customer transactions to a random Vanguard, customer, who was not associated with the 71 Vanguard customers. The customer who received the 71 emails tweeted about the incident as follows:

A Vanguard spokeswoman told the Street.com (which broke the story) that the incident was "a one-time, isolated matter" due to a "system error" and that the e-mails contained *merely* names and transaction confirmation details. Not very illuminating or particularly comforting.

Vanguard's flawed response demonstrates how, too often, SEC-registered entities can underestimate just how difficult it is to manage customer data-related predicaments, whether the result of breaches or technical glitches.

For financial firms like Vanguard, the mishandling of any sort of data mishap can trigger for-cause regulatory examinations; state and federal investigations; customer class actions; and innumerable unintended consequences. Moreover, the enhanced regulatory scrutiny—together with the typically unfavorable media coverage following any sort of customer data mishap—can lead to investor flight, management shake-ups, and even C-suite firings.

From the instant a firm first becomes aware of a customer data issue, every step that follows, especially for an SEC registered entity, must be taken lawfully, meticulously, professionally, and consistent with the highest ethical standards. Below are some imperatives, not just for surviving a customer data crisis, but also for emerging stronger, healthier, and more successful than ever.

The SEC and cyber-security. Cyber-security at SEC-registered entities like Vanguard has become a top priority for the SEC. On Sept. 15, 2015, the SEC announced its second sweep of brokerage and advisory firms' cyber-security practices. Specifically, in an SEC Risk Alert, the SEC's Office of Compliance, Inspections, and Examinations (OCIE), in an unprecedented move, published its actual cyber-security examination "module" (a five-page exhaustive questionnaire) for use during its sweep. This second SEC sweep comes exactly 17 months after the the agency's first sweep in 2014, which contained a similarly comprehensive examination "module."

The first SEC sweep, a mission more akin to reconnaissance than investigation, sought a better understanding of: (1) the cyber-security risks in the securities industry; and (2) how firms were preparing for and responding to these risks. It also plainly marked cyber-security as SEC territory. With the announcement of the second sweep, the gloves clearly came off, and the SEC reinforced its commitment to policing cyber-security at registered firms.

Every SEC-registered firm, including Vanguard, must recognize the SEC's increasing commitment to regulating cyber-security and be sure to investigate data mishaps above all else, with independence and neutrality.

Independence and neutrality. It is difficult to characterize tech mishaps with any sort of terminology (whether negligent, reckless, or intentional), and Vanguard's account of its incident as a "system error" could mean anything. Investors, customers, regulators, law enforcement, partners, employees and just about every conceivable constituency will be unsatisfied with Vanguard's response. The release of private customer financial data is grave and, without further information from Vanguard, no one will believe that their incident response was a minor fluke, merely because Vanguard says so. There are too many outstanding, unanswered questions.

Related articles

The SEC's Newly Proclaimed Search Warrant Authority (http://www.complianceweek.com/blogs/john-reed-stark/the-sec%E2%80%99s-newly-proclaimed-search-warrant-authority)

What Makes a Good 'Pen Tester' (http://www.complianceweek.com/blogs/john-reed-stark/what-makes-a-good-%E2%80%98pen-tester%E2%80%99)

Transforming the Cyber-Security Paradigm (http://www.complianceweek.com/blogs/john-reed-stark/transforming-the-cyber-security-paradigm)

Vanguard customers whose information was compromised will need more detail. Moreover, the SEC will want to know precisely what occurred—e.g. was the "system error" due to an internal controls weakness? Human error? Software bug? How does Vanguard test these systems, and why did the testing not identify the weakness? Did any auditor probe the event?

To handle this matter appropriately: (1) Vanguard's board should engage a former SEC senior official from an independent and neutral law firm (never engaged before) together with a digital forensics firm to conduct an investigation and report its findings to the board; (2) Vanguard should report the investigation's progress to the SEC every step of the way; and (3) Vanguard should disclose the details of the incident to those persons compromised. Instead of trying to characterize the mishap, Vanguard should simply state that it has undertaken the above actions, which evidence strong corporate ethics; fierce customer dedication; and steadfast corporate governance.

Remarkably, so many financial firms fail to grasp the critical necessity for independence. Having the same internal team that is responsible for data security also investigating a data security failure is an inherent (and obvious) conflict of interest. Strong corporate leaders seek answers from independent and neutral sources of information. Otherwise, risks are not properly exposed and examined, and they become exacerbated rather than assuaged.

Counsel as quarterback. The GC is the most logical and effective choice to quarterback a company's response to a data mishap, because the legal ramifications of any failure can be calamitous or even fatal, especially for SEC-registered entities. Just like any other internal investigation, the work relating to a data problem is rife with delicate and complex legal issues, ranging from regulatory inquiries to customer class actions. By leading investigative workflow, GCs can command the investigation and remediation for the C-suite and share with senior management the ultimate responsibility for key decisions.

Additionally, after any episode where customer data security has been compromised, customers, partners, regulators, law enforcement agencies, and others may request copies of investigative reports, forensic images of relevant systems, names of potentially aggrieved parties, employee interviews, etc. These requests raise a host of legal issues, including whether providing the information could violate the privacy of customers or result in a waiver of the attorney-client privilege.

Whistleblowers and social media. No company can sweep data problems under the rug. Whether orchestrated by cyber-attackers, former or current employees, or outsiders, data compromises will always come to light, be it on social media like Twitter or, more likely, in a whistleblower complaint to the SEC.

Whistleblower laws have particularly empowered even the most low-level IT personnel to report any cyber-security concerns. Specifically, the whistle-blower provisions of the Dodd-Frank Act reward informants who provide actionable information with between 10 and 30 percent of any follow-up SEC recovery over $1,000,000. No financial firm is immune to employees (and others) who are economically incentivized to report even baseless allegations to the SEC (and send them electronically and anonymously if they so choose). This is why firms like Vanguard should disclose problems to the SEC early and fully. The SEC is eventually going to find out one way or another; better to get out in front than play catch-up.

The R.T. Jones matter. R.T. Jones, a St. Louis-based SEC-registered investment adviser, stored sensitive personal data of clients and others on its third-party-hosted web server from September 2009 to July 2013. In July 2013, an unknown hacker gained access to the firm's web server, rendering the personal data of more than 100,000 individuals, including thousands of R.T. Jones's clients, vulnerable to theft. The SEC charged that R.T. Jones failed to conduct periodic risk assessments, implement a firewall, encrypt PII stored on its server, or maintain a response plan for cyber-security incidents, and R.T. Jones simultaneously settled, an administrative action relating to the failures. The settled SEC order provides two important lessons for firms experiencing a customer data crisis.

First, breached investors (i.e., customers whose data *may* have been compromised) need not suffer any harm in order for the SEC to bring charges. Just like many of the more notorious data breaches, in R.T. Jones: (1) no one could identify the actual perpetrator of the data breach; and (2) actual harm to customers is presumed. Based on Vanguard's statement implies "no harm, no foul," which in addition to being a poor PR strategy, is also irrelevant.

Secondly, the detailed list of mitigating factors contained in the SEC's R.T. Jones administrative papers, offer an implicit promise that good regulatory behavior after a data mishap can mitigate culpability and, in the right circumstances, perhaps even help a company avoid an SEC enforcement action altogether.

Remedial actions cited by the SEC in the R.T. Jones matter include: (1) the appointment of an information security manager to oversee data security and protection; (2) the adoption and implementation of a written information security policy; (3) the retention of a cyber-security firm to provide ongoing reports and advice on the firm's information; (4) the swift hiring of an outside and independent consulting firm to investigate the data breach; and (5) the prompt notice and free identity theft monitoring provided to those individuals whose information may have been compromised.

Conclusion. Data security issues can happen anytime and remain an unfortunate fact of life for every business, especially SEC-registered entities. Consequently, what's most important is often the response to a mishap rather than the mishap itself. So many companies fail to appreciate this subtle but critical notion. Indeed, if handled correctly, a customer data compromise like Vanguard experienced can actually evolve into a successful failure that not only strengthens cyber-security infrastructure, but also reinforces a firm's commitment to customers, partners, and other fiduciaries. Ironically for Vanguard, the company's data problem created such an opportunity; the response team just missed it.