Published on *The National Law Review* https://natlawreview.com

Timing Is Everything in Data Breach Investigations and Disclosures: Yahoo Breach

Article By:

Kurt R. Hunt

In *cybersecurity*, it's best to learn from others' mistakes. Every company now has an opportunity to learn a lesson that ***Yahoo*** might have to learn the hard way: delays in discovering, investigating, and disclosing data breaches can cause huge problems.

Yahoo recently announced the compromise of more than 500 million user accounts in what appears to be the largest reported data breach in history. Experts have opined on several potential fallouts from the breach, including the possible collapse of Verizon's $4.8 billion bid to purchase Yahoo and the end of the Web's reliance on passwords and security questions. But it's the timing of Yahoo's actions that may prove to be the most instructive aspect of this breach.

Although the data breach reportedly occurred in late 2014, it was allegedly not discovered until the summer of 2016 and not made public until September 2016. The public announcement came just two months after Yahoo announced Verizon's bid to buy its operating assets, and mere weeks after Yahoo reported to the Securities and Exchange Commission that it knew of no incidents of unauthorized access of personal data that might adversely affect the proposed acquisition.

Members of U.S. Congress have referred to the apparent delays as "unacceptable," and at least one senator has requested an investigation by the SEC, raising the possibility that Yahoo has not fully complied with the *SEC's 2011 Guidance Concerning Cyber Security Incident Disclosure*.

Whatever the outcome for Yahoo, the events serve as a reminder to all companies: when it comes to data breaches, delay – or even the perception of delay – can dramatically increase risks and can draw increased scrutiny from regulators, press, and potential plaintiffs.

Happily, companies can take several measures to help guard against such costly delays:

- Detect – Implement comprehensive and rigorous written information security policies containing monitoring requirements, periodic technical assessments, and other measures that will help ensure your company detects data breaches in a timely manner.

- Respond – Prepare your incident response plan before the emergency strikes. Be sure it enables your response team to swiftly investigate, respond, and resolve incidents. Taking the

weekend off after a potential breach might be the difference between a false alarm and the front page.

- Special Cases – Companies in regulated industries, sensitive public relations situations, or pivotal business maneuvers (such as mergers and acquisitions) should ensure that these special circumstances are appropriately addressed in their incident response policy. Perceptions of negligence or dishonesty can cause an already-difficult situation to rapidly deteriorate.

In short: prepare in advance and stay vigilant. Paying attention to your company's cybersecurity posture and being mindful of the urgency of cybersecurity compromises can help your company avoid being the next Yahoo.

National Law Review, Volume VI, Number 307