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

Yes, You Can Face Prison Time For Hiding A Data Breach

By **Ben Kochman**

Law360 (October 6, 2022, 10:04 PM EDT) -- Former Uber security chief Joseph Sullivan's conviction on charges of covering up a 2016 data breach and his potential sentence of up to eight years in prison drive home the importance of speaking frankly within C-suites and with regulators about cybersecurity episodes.

The impact of Sullivan's guilty verdict Wednesday — marking the first time a company executive has been found guilty of covering up a data breach — will be deeply felt at businesses across the globe, attorneys and cybersecurity experts told Law360 on Thursday.

"When a company is under a cyberattack, the pressure and demands upon tech personnel can become overwhelming, and it can be tempting to try to cover up what could be perceived as mistakes," said John Reed Stark, a veteran data breach response and digital compliance adviser. "The lesson here is one of transparency, candor, honesty and immediate communication of critical details up the chain of command."

Certain elements of Uber's mishandling of the breach, described in detail during a **four-week trial** in California federal court, are unique to Sullivan's case, including the former chief security officer's effort to conceal the episode from investigators at the Federal Trade Commission, which at the time was investigating what agency officials have called a "strikingly similar" 2014 data breach at Uber.

But other parts of the case — in which two men extorted the company into paying them $100,000 after stealing data affecting 57 million Uber passengers and drivers — should be familiar to breach responders who deal with ransomware groups that increasingly have turned to data theft and extortion as part of their toolbox.

Such attacks have become far more commonplace in the years since Sullivan made the payoff to Vasile Mereacre and his partner Brandon Glover, who had discovered an Uber security flaw that allowed them access to the company's cloud-stored database.

Uber's management initially attempted to handle the 2016 incident though its "bug bounty" program, which is typically used to compensate cybersecurity researchers who report security flaws to the company. But the $100,000 sum paid to Mereacre and Glover was 10 times the program's award cap at the time, and Uber executives **later admitted** that the payoff was akin to extortion.

Mereacre and Glover, who **pled guilty** to federal charges stemming from the case, were asked by Sullivan to sign a nondisclosure agreement falsely stating that they did not "take or store any data," **Mereacre testified** during the trial.

Sullivan also kept the episode a secret from Uber's general counsel Salle Yoo, as well as the company lawyers assigned to work on the FTC investigation, all the while signing off on documents going to the FTC that he knew were misleading, according to the government.

"The evidence elicited by prosecutors in this case show that Sullivan took several affirmative actions that supported the obstruction and misprision charges, and which set this situation apart from a typical incident response," said Myriah Jaworski, a member of the data privacy and cybersecurity team at Clark Hill PLC.

"This should not be an existential crisis for CISOs and security professionals," Jaworski added, referring to chief information security officers. "Sullivan's actions were irregular."

Sullivan, a former federal prosecutor and internet security expert who months before the 2016 incident had been tapped by then-President Barack Obama to join his administration's national cybersecurity commission, now faces a maximum of eight years in prison and possibly hundreds of thousands of dollars in fines at sentencing, according to the government's penalty filing.

Uber, meanwhile, escaped the FTC investigations into both the 2014 and 2016 incidents without paying a **single cent** in fines, although the company later agreed to pay $148 million in a **joint settlement** with the top law enforcement officers of all 50 U.S. states stemming from the cover-up.

Arsen Kourinian, a partner in the cybersecurity and privacy practice at Mayer Brown LLP, said Thursday that "the charges and ultimate verdict are not a surprise," given what he called a "growing trend in the United States to hold officers and directors of companies personally liable" for failing to be truthful about data privacy and security incidents.

"What was a surprise was that criminal charges were brought, instead of the more common civil lawsuits," Kourinian noted.

Brett Callow, a threat analyst with New Zealand-based cybersecurity company Emsisoft, which tracks the spread of ransomware attacks, said he believes other company officials who may have hidden data breaches from authorities in the past will take notice of Sullivan's conviction.

"It would be very naive to believe that other executives haven't done the exact same thing that Joe Sullivan is alleged to have done," Callow said. "I'm sure that some people will be sleeping less well as a result of the guilty verdict."

--Additional reporting by Bonnie Eslinger. Editing by Jill Coffey and Alanna Weissman.
