LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
TUESDAY, JANUARY 10, 2023

PERSPECTIVE

Uber scrutiny of cybersecurity

By Jennie Wang VonCannon

Joe Sullivan, the former head of security at Uber, leaves court in San Francisco on Friday, Sept. 16, 2022
New York Times News Service

Joseph Sullivan became a cautionary tale in the cyber security community in October 2022 by having the dubious honor of being the first Chief Security Officer (CSO) of a major public company to be convicted of a crime stemming from a data security breach at the company.

A federal jury in the Northern District of California convicted Sullivan, the former CSO of Uber Technologies, Inc. (Uber), of obstruction of justice and misprision of felony (failing to report knowledge of the commission of a felony) for "his attempted cover-up of a 2016 hack of Uber." (U.S. Attorney's Office for the Northern District of California Press Release, Oct. 5, 2022) (USAO Press Release).) Many of the particulars of Sullivan's conduct read like they came from a "what not to do in the event of a data breach" manual – including using a bug bounty program intended for "white hat" hackers who help companies shore up their cyber defenses to pay malicious actors ransoming the company ten times the amount authorized by the program (Perlroth, Nicole and Isaac, Mike, "Inside Uber's $100,000 Payment to a Hacker, and the Fallout," The New York Times, Jan. 12, 2018); hiding a massive data breach from the Federal Trade Commission, which was in the midst of investigating the company for its handling of a prior data breach (USAO Press Release); and lying to the company's CEO and outside counsel about it (*id.*). Sullivan's conviction has also struck fear in the hearts of executives throughout corporate America, because now the specter of criminal liability for near-inevitable data security hacks is on the table if such breaches are not handled properly. And because the Sullivan case is on the extreme end of what not to do, it does not give corporate executives and leaders much guidance on what they *should* do before, during, and after a cyber incident.

This is particularly anxiety-inducing because 2022 could be heralded as the year that lawmakers and regulators doubled down on increasing requirements for transparency and accountability with respect to data breaches and ransomware attacks. Sullivan's conviction came just seven months after President Joe Biden signed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 into law in March – which will eventually require all "covered entities" within sixteen broadly-defined critical infrastructure sectors to notify the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours of suffering a "covered cyber incident," or within 24 hours of making a ransomware payment once CISA implements its Final Rule. (Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).) Also in March, the Securities and Exchange Commission (SEC) proposed a new cybersecurity rule that will, among other things, require public companies to disclose "material" cyber incidents within four business days of discovery, be transparent about

Jennie Wang VonCannon *is a partner at Crowell & Moring LLP.*

their cybersecurity risk management policies and procedures, and disclose their boards' oversight of and expertise in cybersecurity. (SEC Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Proposed Rule, Mar. 9, 2022.) While not finalized yet, the SEC rule is just one more data point evidencing that cybersecurity is now, more than ever, a matter that both public and private companies alike should take seriously.

So what is a C-suite executive, General Counsel, or board member to do?

Remember that the name of the game is resilience. What that means in the cybersecurity context is that in the face of near-certain odds that a company is going to get hacked, it behooves its leaders to think in terms of being proactive and agile – not just focusing on survival. It is not unlike earthquake preparedness: California is overdue for "The Big One" and experts continuously recommend certain measures to prepare for an inevitable earthquake. Those lessons can be carried over into the corporate cybersecurity world.

First, a company needs to have a plan of action for a cyber attack, often called an incident response plan. Depending on the size, sophistication, and resources of the company, this can be as bare-bones as "call the cyber insurance company," or be granular and consist of a written plan detailing how the company's information technology (IT) infrastructure is set up to detect breaches, who will be notified of one and when and how, differing responses to the various types of breaches, etc. The more detailed the plan the better, because it not only gives the leaders of the company a roadmap for what to do during a cyber incident, it can also shed light on individuals who are not following the predetermined protocol and thereby enabling executives to address deviations before they become serious enough to warrant regulatory scrutiny or criminal prosecution. An incident response plan created *before* a data breach is an invaluable guide during an incident, when panic can ensue and judgment can become impaired because the stakes can be very high for a company when its invaluable data is rendered inaccessible or at risk of being publicly disclosed.

This is why once an incident response plan is in place, the company should stick to it – taking into account contingencies that were not anticipated, of course. A careful balance must be struck between agility and trusting the judgment of the cooler heads that created the plan. And, once the immediate period of urgent response has passed and the company has a chance to regroup, company leaders should conduct an after-action debrief, assess what worked and did not, and update the incident response plan accordingly.

Finally, when it comes to disclosing the existence of a cyber incident, company leaders need to keep in mind their increasingly broad obligations to be transparent to myriad constituencies, including their customers, their shareholders, state attorneys general, and the federal government – to name just a few. Failure to do so can lead to fines, class action lawsuits, and – as the Sullivan case shows – possible criminal prosecution.