"All the News That's Fit to Print"

The New York Times

VOL. CLXVII .... No. 57,841 SATURDAY, JANUARY 13, 2018

11

Nicholas Schiedop

'Bug Bounties' Under Scrutiny After Uber Quietly Paid Hacker

By NICOLE PERLROTH and MIKE ISAAC

SAN FRANCISCO — "Hello Joe," read the November 2016 email from someone identifying himself as "John Doughs." "I have found a major vulnerability in Uber."

The email appeared to be no different from other messages that Joe Sullivan, Uber's chief security officer, and his team routinely received through the company's "bug bounty" program, which pays hackers for reporting holes in the ride-hailing service's systems, according to current and former Uber security employees.

Yet the note and Uber's eventual $100,000 payment to the hacker, which was initially celebrated internally as a rare win in corporate security, have since turned into a public relations debacle for the company. In November, when Uber disclosed the 2016 incident and how the information of 57 million driver and rider accounts had been at risk, the company's chief executive since August, Dara Khosrowshahi, called it a "failure" that it had not notified people earlier. Mr. Sullivan and another colleague were fired.

In the weeks since, Uber's handling of the hacking has come under major scrutiny. Not only did Uber pay an outsize amount to the hacker, but it also did not disclose that it had briefly lost control of so

Continued on Page A15

'Bug Bounties' Scrutinized After Uber Secretly Paid $100,000 to a Hacker

From Page A1

much consumer and driver data until a year later. The behavior raised questions of a cover-up and whether the payment really was just a ransom paid by a security operation that had been left alone to act on its own for too long.

The hacking is now the subject of at least four lawsuits, with attorneys general in five states opening investigations into whether Uber broke laws on data-breach notifications. In addition, the United States attorney for Northern California has begun a criminal investigation into the matter.

Most of all, the hacking and Uber's response have fueled a debate about whether companies that have crusaded to lock up their systems can scrupulously work with hackers without putting themselves on the wrong side of the law.

Uber is illustrative of a breed of company that aimed to bulletproof its security. While many corporations were for years blissfully unaware of hackers penetrating their systems, Uber and others recruited former law enforcement and intelligence analysts and installed layers of technical defenses and password security. They joined other companies in embracing the same hackers they once treated as criminals, shelling out bug bounties as high as $200,000 to report flaws.

Yet since the fallout from Uber's disclosure, Silicon Valley companies have taken a harder look at their bounty programs. At least three have put their programs under review, according to two consultants who have confidential relationships with those companies, which they declined to name. Others said criminal prosecutions for not reporting John Doughs would deter ethical hackers who would otherwise come forward, causing even more security breaches.

"Anything that causes organizations to take a step backwards and not welcome contributions from the security community will have a negative impact on all of us," said Alex Rice, a co-founder of HackerOne, a security company whose business is to work with customers, including Uber, to manage interactions with and payments to hackers.

The situation is complicated by Uber's track record for pushing boundaries, which put it under scrutiny last year and helped spur the resignation of Travis Kalanick, its longtime chief executive, in June. Mr. Khosrowshahi has since vowed to change the way the company conducts itself.

This account of Uber's hacking and the company's response was based on more than a dozen interviews with people who scrambled to deal with the incident, many of whom declined to be identified because of the confidentiality of their exchanges. Many are current or former members of Uber's security team, who defended their actions as a prime example of how executives should respond to security problems in their systems. The New York Times also obtained more than two dozen internal Uber emails and documents related to the incident.

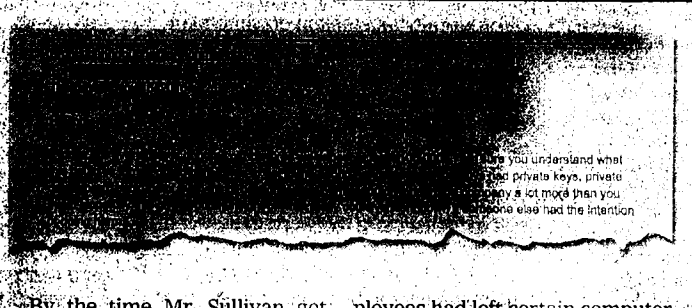
In a statement, Mr. Sullivan disputed the notion that the 2016 episode was a breach and said Uber had treated it as an authorized vulnerability disclosure.

"I was surprised and disappointed when those who wanted to portray Uber in a negative light quickly suggested this was a cover-up," he said, adding that he was proud its engineers had been able to fix the issue before it could be abused. He declined to discuss disclosure because of the active state investigations.

Matt Kallman, an Uber spokesman, said, "We stand by our decision to very publicly disclose the 2016 data breach — not because it was easy, but because it was the right thing to do."

Through a spokesman, Mr. Kalanick declined to comment.

Uber started its bounty program in March 2016, challenging hackers to find bugs that could specifically lead to the exposure of sensitive user data. The higher risk the bug was, the more Uber would pay. In Uber's calculus, the payouts were better than learning about a vulnerability only after attackers had abused it.



DAVE SANDERS/FOR THE NEW YORK TIMES

A hacker told Uber of a major vulnerability in November 2016. The company disclosed the breach a year later. Left, an email from "John Doughs."

By the time Mr. Sullivan got John Doughs email, Uber had paid rewards to hundreds of hackers. Mr. Sullivan forwarded the John Doughs note to his team for vetting and, if all checked out, patching and payment.

Uber's security team used nicknames for hackers, particularly the colorful, anonymous ones who engaged with the company. John Doughs was called "Preacher" for his admonitions that Uber should be better at security.

"It's very disappointing to be finding this vulnerability in such way," the hacker wrote in an email to Rob Fletcher, Uber's product security engineering manager. "Especially coming from a company like Uber."

Other emails obtained by The Times show Mr. Fletcher treated the incident as a bounty and encouraged Preacher to provide proof of the vulnerability, including sending a few lines of data from the database he had breached.

According to the emails obtained by The Times, Uber soon discovered that some of its employees had left certain computer code known as keys on a programming site called Github. Those keys had allowed Preacher to gain access to Uber's Amazon web servers, where it stored source code as well as 57 million customer and driver accounts, including drivers license numbers for some 600,000 Uber drivers. It was a major oversight. To fix it, Uber had to inform everyone at the company that it was temporarily shutting down access to Github.

Emails between the hacker and Mr. Fletcher continued. In some, Mr. Fletcher thanked the hacker for helping the company fix the oversight. In two emails, Preacher's motivations appeared to veer closer toward blackmail. In one, he demanded "high compensation" for his findings. After Mr. Fletcher wrote that the company's maximum bounty was $10,000, Preacher said he and his team would only accept "six digits."

Mr. Fletcher said he would need to seek authorization for a $100,000 payment, and would need Preacher's reassurances that he would delete the data he had downloaded. Mr. Fletcher also pushed the hacker to take payment through HackerOne, which requires bounty recipients to disclose their real identities for tax requirements.

Mr. Fletcher drew further details about the hacker out through emails, including tidbits about his identity, his internet hosting provider, the location of his computer and proof that he deleted his copy of Uber's downloaded data.

According to the emails, Uber at one point extended Preacher an all-expenses paid trip to San Francisco, where the company is based. Uber asked the hacker to discuss his security techniques and offered to introduce him to companies that might be interested in his skills. Preacher declined.

By then, Uber's executives had made their decision about what to do. Mr. Kalanick signed off on the $100,000 payment, so long as the hacker signed an agreement to destroy any data exposed in his discovery, according to the emails.

Preacher's trail of digital bread crumbs eventually led to a 20-year-old whose first name was Brandon and who was living in a Florida trailer park with his fam ily, according to the emails. It wa there that Brandon signed agree ments assuring Uber that he ha deleted the data he had down loaded.

The Times was unable to lear Brandon's full name. An email t the John Doughs account bounce back.

Uber's security team was soo celebrating its response to wha could have been a major securit breach. Mr. Sullivan and his co leagues were praised in year-en performance reviews, includin by Mr. Kalanick, according to cur rent and former employees.

What is now at issue is whethe Uber executives broke the law with the $100,000 payment an should have quickly notifie customers or officials of the dis covery. The issue is not legall clear cut.

Laws concerning bug bountie — particularly those that let hack ers view or save sensitiv customer data — are ambiguous The Justice Department weighe into bug disclosure programs fo the first time in July and largely left it to organizations to decid what access they will authorize for hackers and what they can d with the data. In Uber's case, it bounty guidelines authorized an encouraged hackers to look fo vulnerabilities that exposed it most sensitive user data.

Breach disclosure laws also dif fer state to state. The state laws most relevant to Uber's case re quire disclosure if names are ex posed in combination with driv er's license numbers in a "breach of security."

Brandon received two pay ments of $50,000 each from Uber on Dec. 8, 2016, according to the emails. Uber continued trading emails with Brandon during 2017, until the conversation eventually dwindled.

The matter seemed settled — until Mr. Sullivan received a phone call while preparing Thanksgiving dinner, according to two people familiar with the matter. He was being fired, effective immediately, for failing to disclose the incident to the proper authorities at the time.

Fueling a debate in Silicon Valley over how companies deal with security threats.