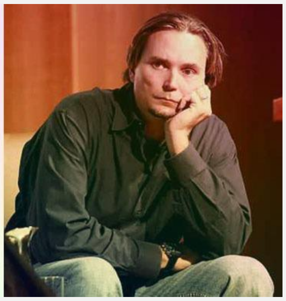
Ransomware Payout, Coverup, & Prison Potential



Joe Sullivan, a prominent security expert, spent the first eight years of his career working for the Department of Justice, first as an intern at the DOJ Miami office. He prosecuted cybercrimes for the San Francisco U.S. attorney's office, working with Robert Mueller, then as Assistant United States Attorney at the District of Nevada in Las Vegas, and worked as Assistant US Attorney at the Northern District of California. Sullivan was the top security officer at Facebook, Uber, and Cloudflare, and a Commissioner for Obama Cyber Commission. Next, he faced his previous employer U.S. attorney's office – this time as a defendant charged with obstruction of justice for concealing a 2016 breach of Uber customer and driver records from the Federal Trade Commission and for actively hiding a felony.

Sullivan authorized payments to hackers after the 2016 breach, using Bug Bounty money to make a $100k ransomware payment.

The jury rendered a unanimous verdict, finding him guilty of both charges. Sullivan faces a five-year prison sentence on the obstruction charge, three years for failing to report a felony, and fines of $500k.

This case is the first major criminal case brought against a corporate executive over a breach by outsiders. However, payoffs to extortionists, including those who steal sensitive data, have become so routine that some security firms and insurance companies specialize in handling the transactions. "Paying out the ransom I think is more common than we're led to believe. There is an attitude that's similar to a fender bender," said Michael Hamilton, founder, Critical Insight.

FBI leaders have vocally discouraged paying ransoms but have said they will not pursue the people and companies that pay ransoms as long as they don't violate sanctions prohibiting payments to named criminal groups especially close to the Russian government.

States typically require companies to disclose breaches if hackers download personal data and a certain number of users are affected. There is no federal law requiring companies or executives to reveal breaches to regulators. Federal officials have pressed for recent legislation that will require ransomware notifications from critical infrastructure victims to the Cybersecurity and Infrastructure Security Agency. The Securities and Exchange Commission is also pushing for more disclosure.

The Federal Trade Commission deposed Sullivan as part of their investigation of a 2014 breach of Uber's online systems. Ten days later, a hacker emailed Uber and described a security lapse that allowed him and a fellow hacker to download data using a digital key Uber had left exposed to get into an Amazon account and download the personal data of about 600,000 Uber drivers and additional personal information associated with 57 million riders and drivers. Uber did not publicly disclose the incident or inform the FTC until a new chief executive, Dara Khosrowshahi, joined the company in 2017.

The hackers demanded a ransom in exchange for destroying the data. Sullivan's team said they could pay under Uber's bounty program but that the top payout under it was $10k. The hackers said they would need at least $100k Sullivan paid a $100k ransom payment and had the hackers sign a nondisclosure agreement. The hackers were later arrested and pleaded guilty to hacking charges, and one testified for the prosecution in Sullivan's trial.

Federal prosecutors presented evidence that "after Uber personnel were able to identify two of the individuals responsible for the breach, Sullivan arranged for the hackers to sign fresh copies of the non-disclosure agreements in their true names. The new agreements retained the false condition that no data had been obtained. Uber's new management ultimately discovered the truth and disclosed the breach publicly, and to the FTC, in November 2017." They argued that Mr. Sullivan knew that revealing the new hack would extend the FTC investigation and hurt his reputation. "He took many steps to keep the FTC and others from finding out about it," Benjamin Kingsley, an assistant U.S. attorney, said during closing arguments. "This was a deliberate withholding and concealing of information."

"This case will certainly make executives, incident responders and anybody else connected with deciding whether to pay or disclose ransom payments think a little harder about their legal obligations. And that's not a bad thing," said Brett Callow, threat analyst at Emsisoft. "As is, too much happens in shadows, and that lack of transparency can undermine cybersecurity efforts."

Prosecutors argued in Sullivan's case that his use of a nondisclosure agreement with the hackers was evidence that he participated in a coverup. They said the break-in was a hack that was followed by extortion as the hackers threatened to publish the data they took, and so it should not have qualified for Uber's bug bounty program to reward friendly security researchers. But the reality is that as the hacking of corporations has gotten worse, the way companies have dealt with it has moved far past the letter of the law when Sullivan was accused of breaking it.

The conviction stunned corporate security and compliance members. While Sullivan directed the response to the two hackers, many others at the company were in the loop, including a lawyer on Sullivan's team, Craig Clark. Evidence showed that Sullivan told Uber's CEO, Travis Kalanick, within hours of learning about the threat himself, and that Kalanick approved Sullivan's strategy.

Most security professionals had been anticipating Sullivan's acquittal, noting that he had kept the CEO and others who were not charged informed of what was happening. "Personal liability for corporate decisions with executive stakeholder input is a new territory that's somewhat uncharted for security executives," said Dave Shackleford, Principal Consultant, Voodoo Security. "I fear it will lead to a lack of interest in our field, and increased skepticism about infosec overall."

Ransomware attacks were rare when Sullivan was charged but have increased dramatically in the last couple of years. The techniques in those attacks have also shifted. At the beginning of 2020, most ransomware merely encrypted files and demanded money for the key to unlock them. By the end of that year, most ransom attacks included the outright theft of files, setting up a second ransom demand to prevent their public release, according to a 2021 report by the Ransomware Task Force, an industry-led group that includes representatives from the U.S. Cybersecurity and Infrastructure Security Agency, the FBI, and the Secret Service. More recently, cryptocurrency exchanges have been robbed and then negotiated to give massive payments to get those funds back.

"Especially over the past six months in the crypto space, the model is 'build it until we get hacked, and we'll figure it out from there,' " said Ellis. As average payouts zoomed past Sullivan's, into the hundreds of thousands of dollars, more businesses turned to insurance companies for predictability. But often, the insurance companies reasoned it was cheaper to pay than to cover the damage from lost files. Some paid regularly, ensuring steady earnings for the gangs. Making payments illegal, as some have proposed, would not actually stop them, the FBI has said. It would instead give the extortionists yet another club to hold over their victims after payment is made. At least so far, Congress has agreed, declining to ban the transactions.

After Kalanick was forced out of the company for unrelated scandals, his replacement, Dara Khosrowshahi, came in and learned of the breach. Sullivan described it as a routine payoff but a later investigation turned up the full story, and Khosrowshahi fired Sullivan for not telling him more, sooner. Uber helped the U.S. attorney's office build their case against Sullivan.

Sullivan did not reveal the 2016 hack to Uber's general counsel but he did discuss it with Uber lawyer, Craig Clark. Like Sullivan, Clark was fired by Khosrowshahi after the new chief executive learned about the details of the breach. Clark was given immunity in exchange for testifying against Sullivan. Clark testified that Sullivan had told the Uber security team that they needed to keep the breach secret and that Sullivan had changed the nondisclosure agreement signed by the hackers to make it falsely seem that the hack was white-hat research. According to Clark, Sullivan said he would discuss the breach with Uber's "A Team" of top executives. Sullivan only told CEO, Travis Kalanick. Kalanick approved the $100k payment to the hackers. Prosecutors unsuccessfully tried to get Sullivan to implicate Kalanick.

Clark acknowledged advising the team that the attack would not have to be disclosed if the hackers were identified, agreed to delete what they had taken and could convince the company that they had not spread the data further, all of which eventually came to pass. Prosecutors were left to challenge "whether Joe Sullivan could have possibly believed that" as one of them put it in closing arguments.

Accountability for the payoff and coverup, but not for sloppy security…

There is information that an 18 year old breached Uber's network a couple of weeks ago by tricking an employee to give their login credentials by pretending to be a colleague. The hacker posted company-wide on Slack regarding the breach and the boast posts were so brazen that employees thought the entire incident was a joke. The hacker described Uber security as "awful." Screenshots included proof that the hacker had access to highly privileged security accounts, which would provide wide authority inside the company. Uber included passwords in programs used for accessing key outside resources, such as Amazon Web Services, so the hacker did not need to break into more exclusive internal accounts or even guess.