Research Note

#DeleteUber

Lee Segal

Published: February 2019
Written: March 2018

Keywords: Uber; Reputational Risk; Cybersecurity; Ethics; Leadership

Abstract: This paper discusses how the disruptive and once innovation company Uber has continued its downward spiral, with a growing number of stories emerging of executives making unethical decisions that will have lasting consequences for the company's reputation and bottom-line. Incidents run the gauntlet from practicing unethical methods of gathering data on competitors; a toxic internal culture that has resulted in numerous sexual harassment and discrimination cases; patterns of exploiting employees; and compromising private customer data access; and failure to secure sensitive private information. Despite leadership changes, Uber has a long way to go to demonstrate they have successfully implemented meaningful and lasting cultural and administrative changes.

In 2010, a revolutionary application came out allowing users to reserve a car – a taxi of sorts - via a smartphone application. No longer did people have to wait outside in extreme weather, fighting others to hail a cab, unsure when one would arrive. Understanding this unfulfilled need and leveraging mobile smartphone and geolocation technology maturity, two innovators created a service that enables users to order a car service based on their exact location.[1] The application has many useful features including informing the rider of expected arrival time, showing the price before the car is called, tracking the driver on a map, and the capability of contacting the driver if the rider forgets any of their belongings in the vehicle. This innovative service is Uber, which quickly became extremely popular: instead of saying "let me hail a taxi," the new phrase is "let's call an Uber." The founder of Uber identified an unfulfilled need and developed a new business model that opened up a brand-new market—the ability to call cars, and eventually food, to their front door in real-time, at any time and from anywhere with just the touch of a button. The idea was gold. Nevertheless, a lack of ethics and morals led the company to turmoil in 2014; since 2014, Uber has been hit with many allegations placing its ethics into question.[2] However, the data breach revealed in November 2017 plunged Uber's reputation to rock bottom. The once-innovative company is now plagued by scandals and eroding customer trust.

Uber dealt with another security and reputation risk long before this data breach occurred. To fully understand Uber as a corporation and understand why this particular data breach enraged both customers and governments, it is essential to analyze Uber's past mistakes. In 2014, Uber was accused of targeting their competitor, Lyft, by booking thousands of fake rides in an effort to cut into Lyft's profits and services.[3] In that same year, Uber was also accused of having a "God View" which allowed Uber employees (managers and executives) to use the information Uber collected from customers—such as their location—unethically.[4] Employees allegedly used the "God View" to impress and entertain friends and associates, demonstrating a blatant misuse of privileged access to private customer data. This specific incident raised privacy concerns and demonstrated a fundamental lack of enforced policies and procedures related to authorization controls and access to customer data. Then in 2015, Uber revealed they had suffered a data breach that affected roughly 50,000 drivers.[5] They concealed this breach for over a year and were fined twenty thousand dollars in New York.[6] Many Uber drivers started protesting, claiming Uber did not care for them. Uber even tried to keep them as contractors to avoid having to pay them employee benefits, and so they could keep cutting their wages, making it hard to make a living, and never told them that their personal information was stolen. More recently, in 2017, accusations of sexual harassment and discrimination toward females in the workplace arose within Uber.[7] Google also sued Uber, accusing them of stealing Google's technology for a self-driving car.[8] The list continues in March of 2017, when Travis Kalanick (at-the-time-CEO of Uber) was caught on camera yelling at his Uber driver after his driver complained about the difficulty of making a living with the company's declining rates.[9] Then in April, news leaked that Uber had a secret program called "Hell" that allowed the company to spy on its rival Lyft to uncover drivers who work for both companies.[10] They used this application to help steer drivers who worked for both companies away from the competitor. In June, an Uber executive obtained the medical records of a woman who was allegedly raped by an Uber driver just to cast doubt onto the rape victim. Uber fired the executive once the press got word of this incident, and the woman later sued the company for violating her privacy rights and defaming her.[11]

These are just the highlights of the allegations against the corporation's corrupt culture, abuse of power, and their lack of security measures and controls. These security breaches and allegations perfectly frame the tone Uber's chief executive officer (CEO) set for the corporation—it has been led without integrity, transparency, good ethics, or honesty. One of the responsibilities of the CEO is to lead the company in the manner expected of the employee to mimic. Analyzing all the actions Uber has taken in the last year, it is clear that the CEO has failed to set an ethical and just tone for his company. These examples prove that the majority of the executives are only concerned with selfish motives such as making money for their corporation, no matter the cost. In fact, the recent data breach—the focus of this paper—further backs Uber's reputation as a corrupt corporation focused on profits at the expense of ethical business practices.

The most recent data breach, and arguably, "Uber's lowest point," was just announced in November 2017.[12] Uber announced that in October of 2016, they had a data breach that affected over 57 million riders and drivers. *Bloomberg Technology* provides a detailed explanation of the hack: two attackers gained access to Uber's private GitHub repository (a digital directory/storage space) where their software engineers shared and updated code. The hackers succeeded in breaking into the repository because of a failure to implement internal controls and security measures. The hackers found login credentials to Uber's Amazon services account; on this account, the hackers found an archive of riders' and drivers' information including email addresses, full names, and phone numbers.[13] Alongside that information, they found up to sixty thousand driver's license numbers. The attackers blackmailed Uber and demanded one hundred thousand dollars.[14] The executives of Uber immediately agreed on the condition of having all stolen information and any evidence of the hack deleted. They even went through the extra effort of tracking down the hackers and making them sign a nondisclosure agreement to ensure they would not leak information about the hack.[15] In fact, Uber took a few actions to try and keep the hack hidden such as using their bug bounty program as a cover up for paying the ransom.[16] Uber has yet to make any apologies or take ownership for their actions even though they committed countless questionable actions. Uber's dealing with this breach further proves that their executives lack integrity, honesty, transparency, and respect when making decisions and representing the enterprise.

There are always consequences involved when a breach takes place; however, the potential consequences for Uber's customers, who remain oblivious of this breach, increased exponentially should the hackers decide to use the stolen information in the future. The 2016 data breach affected the entire user enterprise including the riders and drivers, Uber's corporate reputation, and Uber's executives. The biggest consequence of the data breach is that private information was stolen (names, email addresses, and phone numbers) from fifty-seven million riders and drivers, along with six-hundred thousand driver license numbers. One might question why the information the hackers stole is essential; however, this is the kind of information used to steal identities or commit social engineering attacks. What makes it even worse is that the users had no idea that their information was even stolen for over a year. In this case, or any case where your private information is stolen, ignorance is *not* bliss. Instead of immediately taking necessary steps to mitigate and protect themselves from a potential attack, the riders and drivers were left clueless and defenseless. Not only did Uber hide the attack from them for over a year, they still have not reached out to any affected riders, and have not communicated any plans to do so. The worst part is that Uber failed to even tell their drivers about their attack, which—after a 2014 ruling—are officially considered employees of the company.[17] Uber not only hid information from customers and the government, but also hid information from their own employees.

Even though none of Uber's information got stolen, they are not making it out of this breach unscathed. Uber is being put on blast from the media, multiple governments, their employees, customers, and other individuals. Uber dealt with reputation issues before the breach. But is safe to say that they have reached a new low. They are not only dealing with protests and strikes, but also countless legal suits. The two biggest suits include one with California and one with the FTC (Federal Trade Commission). In 2003, California mandated that businesses and state agencies are required to alert customers if their personal information is exposed in a security breach; since Uber hid this data breach from its customers, including the ones in California, it broke California's regulation.[18] Uber also broke Federal Trade Commission (FTC) policy by asking the Hackers to delete all forensic evidence of the data breach. A representative of the FTC stated, "Uber failed consumers in two key ways: First by misrepresenting the extent to which it monitored its employees' access to personal information about users and drivers, and second by misrepresenting that it took reasonable steps to secure that data." Most executives have worked in well-known companies for at least a decade; they should be familiar with the laws and protocols. Even if they were not, part of their job as leading a company is finding out what the regulation and protocols are in that area as part of decision-making processes. These actions prove that no matter what the executives were involved with in leading this incident, they knew they were committing illegal acts and decided to pursue them anyway. The crimes explained above are two prime examples of Uber executives prioritizing their company over following laws, regulations or corporate ethics.

Over the last couple of years, Uber's actions have concerned the population for many reasons. Uber has a huge issue with not adapting and learning from past mistakes; they would rather sweep issues under the rug than deal with them in an honest and transparent way. Uber also has huge security issues that have not been fixed. (Note: The new Uber CEO claims to be strengthening controls and security measures on their cloud storage services.) An example of Uber's serious security issues where executives failed to learn from past mistakes is the data breach that occurred in 2014. Uber only disclosed that there was a breach in 201, a whole year after the fact. The only difference is that in 2014 hackers stole less data. But the hackers still got away with personal data from roughly 10,000 Uber drivers. The attack vector used in both attacks is essentially the same; in 2014, the hackers broke into Uber's private Github repo after one of the engineers publicly posted the key to their GitHub. Through the repo they gained log-in information to an Amazon S3 Datastore which Uber used to store data in plain text.[19] The FTC recently settled their investigation into security and privacy complaints for the 2014 data breach; just this summer Uber agreed to 20 years of external audits and to abide by various conditions in the consent order.[20] According to TechCrunch, "the FTC consent order settling the 2014 and 2015 complaints prohibited Uber from misrepresenting how it protects the privacy, confidentiality, integrity, and authenticity of any personal information it handles and stores. However, before the ink could dry on that settlement, Uber revealed the 2016 data breach. The fact that Uber allowed both these attacks to happen in a span of a couple of year, raises a lot of questions about their security measures and the controls they have implemented. After the first attack Uber should have increased security, improved employee training, and added policies to prevent a data breach; or at least solve the vulnerability that had been breached once before.

Clearly, they failed to increase security even slightly, not even patching up the vulnerability, which raises the question of whether security is even a priority for the corporation. Another concern is that Uber knew they were in violation of the settlement with the FTC while they were signing the contract with them, once again demonstrating Uber's lack of respect for laws, regulations, integrity, and honesty. They completely lied to the FTC and committed the same crime they committed two years prior. Repeatedly, Uber executives continue to lead the company with a tone of apathy for corporate ethics.

Not just individuals are outraged with Uber's actions. Governments are also taking a stand. Many governments—especially the UK—claim that Uber's behavior is reckless.[21] The governments are retaliating in response. First, the UK's digital minister, Matt Hancock, decided to create a new regulation. The new regulation "would oblige companies to report breaches 'likely to impact on data subjects to the information commissioner within 72 hours of becoming aware of it and in serious cases will also have to notify those affected by the breach'".[22] The US senate is also trying to pass a regulation that about data breaches that failed to pass in 2015. The bill "would make it a crime – punishable by up to five years in prison – for companies to knowingly conceal a breach of customer information."[23] Hopefully this drastically bill will pass to emphasize to corporation like Uber that data breaches need to be told to the authorities immediately to mitigate the consequences of the breach. Some governments are even banning Uber completely, making it illegal for people to work for Uber and for the population to use Uber. Over 10 countries have already banned Uber, with more looking to follow suit.[24]

If you are currently or have ever been an Uber user, you should automatically assume that you have been infected. Uber has not informed users if they were affected by this hack and has not disclosed any plans to inform users; forcing them to trust that Uber successfully deleted the stolen data and implemented security measures to monitor the stolen data. This is extremely unfair considering that Uber has proven repeatedly to not prioritize security or care about their customers. However, there are a couple steps to try to protect personal information. First, change your password right now. Uber should have forced an automatic password reset. However, since they did not, you should immediately change it yourself. Next, delete all credit card information from the application, but do not delete the application itself. Disable anything that can gather information about you such as location services, credit card information, or any addresses you saved on the application. Keep the disabled application so you can monitor it and make sure there is no suspicious behavior occurring on your account. The third recommendation is to closely monitor your bank account. Uber claims that your social security number - if you are a driver - and credit card information were not stolen; however, as proven through their actions, they are not a reliable corporation.

Uber's board is taking some drastic steps to try to fix their reputation and past mistakes. The most essential step Uber took revolves around changing their leadership; with a change in leadership, a new culture can be fostered for the corporation, hopefully leading to a more transparent and ethical company.[25] Uber fired the two individuals in charge of leading the incident, replaced the CISO, and replaced the current CEO.[26] The new CEO, Dara Khosrowshahi, states that he "commit[s] on behalf of every Uber employee that [they] will learn from [their] mistakes." Uber promises to "[change] the way [they] do business, putting integrity at the core of every decision [they] make and working hard to earn the trust of [their] customers." CEO Dara has asked Matt Olsen, founder of a cyber security consulting firm and former general counsel of the National Security Agency and director of the National Counterterrorism Center, to help him think through how best to guide and structure Uber's security teams and processes going forward.[27] Dara also strengthened controls and implemented extra security measures to protect unauthorized access to their cloud data storage accounts.[28] These first two actions show that Dara is raising the priority of security in the company. With new leadership, Uber is taking steps to mitigate their mistakes taken in response to the 2016 data breach. First, they notified all the drivers with stolen driver's license numbers and are offering the infected drivers free credit monitoring and identity theft protection.[29] Even though Uber has still not notified the affected riders, they are monitoring all the affected accounts and have flagged them for additional fraud protection.[30] Uber already stated that they are increasing security measures and strengthening controls. However, another recommendation is to increase employee training. Clearly, Uber's software engineers need some extra guidance specifically on how to secure and share code uploaded to third-party vendor sites. Hopefully, Uber will continue taking steps towards more honorable actions and prioritization of both security and their customers over themselves.

The recklessness of Uber's actions raises concerns for federal, state, and local government agencies and consumers. Having access to so much personal data including location and credit card numbers proves to be a large security risk for both customers and employees. Uber's past actions are a clear indication that they care more about protecting their reputation and revenue over running the business in an ethical and transparent manner. Uber lied in the past about the protection they have for customer-data and allowed employees to access private data for personal use. They have been accused of having a rule-breaking culture, partaking in sexual assault, being unfair to their employees, breaking FTC regulations, breaking California state laws, and are involved in countless civil suites. Until recent leadership changes, Uber has proven itself as an untrustworthy enterprise that uses its power to take advantage of users and drivers and continuously prioritizes itself over others. Even though Uber made many changes and claim that they are "leading their company into a different direction,"[31] it is too soon to say if consumers and employees alike can trust these promises; first, the new leadership must demonstrate through actions that they are truly implementing a cultural and administrative change.

[1] "Finding the Way Creating Possibilities for Riders, Drivers, and Cities." Uber, www.uber.com/our-story/.

[2] Balachandran, Manu. "A timeline of events that led to the downfall of Travis Kalanick at Uber." *Quartz India*. 21 Jun. 2017. Accessed Mar. 2018 <www.qz.com>.

[3] Levin, Sam. "Uber's Scandals, Blunders and PR Disasters: the Full List." The Guardian, Guardian News and Media, 27 June 2017, www.theguardian.com/technology/2017/jun/18/uber-travis-kalanick-scandal-pr-disaster-timeline.

[4] ibid

[5] ibid

[6] ibid

[7] ibid

[8] ibid

[9] ibid

[10] ibid

[11] ibid

[12] Isaac, Mike, et al. "Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data." The New York Times, The New York Times, 21 Nov. 2017. Accessed Mar. 2018 <www.nytimes.com>.

[13] Newcomer, Eric. "Uber Paid Hackers to Delete Stolen Data on 57 Million People."Bloomberg.com, Bloomberg, 21 Nov. 2017. Accessed Mar. 2018 <www.bloomberg.com>.

[14] ibid.

[15] Newcomer, Eric. "Uber Paid Hackers to Delete Stolen Data on 57 Million People."Bloomberg.com, Bloomberg, 21 Nov. 2017. Accessed Mar. 2018 <www.bloomberg.com>.

[16] Isaac, Mike, et al. "Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data." The New York Times, The New York Times, 21 Nov. 2017. Accessed Mar. 2018 <www.nytimes.com>.

[17] Hern, Alex. "Uber Driver Declared Employee as the Company Loses Another Ruling." The Guardian, Guardian News and Media, 11 Sept. 2015. Accessed Mar. 2018 <www.theguardian.com>.

[18] "Data Security Breach Reporting." State of California - Department of Justice - Office of the Attorney General, 14 Sept. 2017. Accessed Mar. 2018 <www.oag.ca.gov>.

[19] Newcomer, Eric. "Uber Paid Hackers to Delete Stolen Data on 57 Million People."Bloomberg.com, Bloomberg, 21 Nov. 2017. Accessed Mar. 2018 <www.bloomberg.com>.

[20] "Uber Settles with FTC over Privacy and Data Security Promises." Consumer Information, 24 Aug. 2017. Accessed Mar. 2018 <www.consumer.ftc.gov>.

[21] Siddique, Haroon, and Shaun Walker. "Uber Hacking: Customers Not at Risk of Financial Crime, Says Minister." The Guardian, Guardian News and Media, 23 Nov. 2017. Accessed Mar. 2018 <www.theguardian.com>.

[22] ibid.

[23] Vaas, Lisa. "Proposed Law Would Jail Execs Who Fail to Report Data Breaches." Naked Security, Naked Security, 4 Dec. 2017. Accessed Mar. 2018 <www.nakedsecurity.sophos.com>.

[24] Rhodes, Anna. "Uber: Which Countries Have Banned the Controversial Taxi App." The Independent, Independent Digital News and Media, 22 Sept. 2017. Accessed Mar. 2018 <www.independent.co.uk>.

[25] Khosrowshahi, Dara. "Uber Newsroom." 2016 Data Security Incident, 21 Nov. 2017. Accessed Mar. 2018 <www.uber.com>.

[26] ibid.

[27] ibid.

[28] ibid.

[29] ibid.

[30] ibid.

[31] ibid.