Uber’s 2016 Data Breach: What Went Wrong

Matthew Thomas

www.linkedin.com/in/matthewthomas-c

July 21, 2025

Analysis of the 2016 Uber Data Breach

Everyone deserves to have their online privacy and security taken seriously and treated as a fundamental right, and all businesses should take measures to protect their customers' data. The goal of this paper is to summarize the events of the 2016 Uber data breach, one of the largest privacy incidents in recent history. This paper will dive into the series of events and system failures that ultimately led to such a substantial data breach, and what steps Uber took to recover. Additionally, this paper will cover what efforts could have been taken to mitigate or prevent the incident and conclude with key takeaways for other organizations looking to prioritize the safety and security of customer data.

Overview of the 2016 Uber Data Breach

On November 21, 2017, Uber's CEO, Dara Khosrowshahi, announced via a newsroom post that he had recently become aware of a data breach affecting more than 600,000 Uber drivers and more than 57 million users. He notes that, at the time of posting, Uber had taken measures to lock down their systems and remove unauthorized individuals. This post, however, came a year after the breach initially occurred and was detected by Uber (Uber Technologies, Inc., 2017). What Khosrowshahi failed to mention in his post is that, while Uber had locked down their systems, they actually paid the individuals who breached them to delete the data they had stolen.

Uber's Disclosure and Immediate Response

To keep the breach from making its way to the public, Uber paid the hackers $100,000 to delete any exfiltrated data. Uber claimed that they had assurances that all customer data was

wiped, and they even fired two individuals—one being their CSO—who were leading their information security initiatives (Frier & Newcomer, 2017). In addition to Uber paying off the hackers, Etherington (2017) claims Uber also asked the hackers to keep quiet about the breach and not bring this event to the public. Uber not only violated basic data storage rules but also failed to disclose the event entirely.

System Failures and Root Causes

After an investigation led by the FTC, three system failures were alleged to have contributed to the breach between 2014 and 2016. Until at least September 2014, Uber did not implement reasonable security training and did not formalize its information security programs. Additionally, until at least November 2016, Uber stored sensitive data in Amazon data centers in plaintext, completely unencrypted. These data centers were accessed multiple times by thieves who obtained access keys from Uber engineers who posted them on GitHub (Federal Trade Commission, 2018). Considering the size of Uber at the time, simple encryption for customer data should have seemed obvious. However, the lack of simple encryption, along with no formal policy standards, appears to be the result of poor leadership. Shortly before the public disclosure of the breach, Bloomberg reported that Uber fired their chief security officer, Joe Sullivan (Frier & Newcomer, 2017).

Mitigation and Prevention Strategies

Two mitigations become immediately apparent after identifying Uber's infiltration. First, Uber should have encrypted all sensitive customer data in transit and at rest. According to the National Institute of Standards and Technology (NIST), data at rest should be protected using

cryptographic mechanisms. Specifically, NIST SP 800-53 Rev. 5, control SC-28(1), states that organizations should "implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest" (National Institute of Standards and Technology, 2020, SC-28(1)). If proper encryption had been used at the time of the breach, it could have prevented attackers from accessing usable data, resulting in any stolen data being essentially useless.

Secondly, proper security awareness training could have advised employees against posting secure database keys online and helped staff recognize signs that systems were breached, leading to a faster and more effective response. Such training not only contributes to quicker incident response but can reduce the likelihood of future incidents. These are just a few examples of mitigations that could've changed the outcome for Uber in 2016.

Outcomes and Regulatory Action

Ultimately, Uber ended up settling with attorney generals across the country and paying out over $148 million due to the mishandling of customer and driver information. Due to the lack of transparency and concealment of the breach for over one year, Uber may also be subject to future penalties up to $41,000 per person for future violations (Federal Trade Commission, 2018). Uber's 2016 data breach is a perfect example of what businesses should not do. While many businesses may not want to spend the time or money properly securing data or put in place policies for proper handling of data, Uber's 2016 breach is a perfect example of what could go wrong. Uber's total losses include financial penalties exceeding $148 million, loss of customer trust, and a stain on their reputation.

Lessons Learned and Recommendations

These failures offer important lessons for organizations across all industries. Uber's 2016 breach is a textbook reason why businesses must prioritize the encryption of sensitive information, formalize employee training, and disclose any events involving customer data in a timely manner. Uber failed to formalize policies and lacked security awareness, which led to vulnerabilities that exposed customer information to risk. Customers deserve to have their online presence protected just as much as their privacy and security in the physical world. As technology continues to advance and data breaches become more common, organizations can no longer afford to treat cybersecurity as an afterthought. Investment in security not only protects customers but also builds long-term trust and safeguards a company's reputation.

Key Takeaways

- Encrypt sensitive customer data at rest and in transit.
- Provide ongoing security training for all employees.
- Establish and enforce robust data handling and disclosure policies.
- Report breaches promptly and be transparent to customers and authorities.

References

Federal Trade Commission. (2018, October 26). Federal Trade Commission gives final approval to settlement with Uber. https://www.ftc.gov/news-events/news/press-releases/2018/10/federal-trade-commission-gives-final-approval-settlement-uber

Federal Trade Commission. (2018). Uber Technologies, Inc.; Analysis of proposed consent order to aid public comment. https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_revised_analysis.pdf

Frier, S., & Newcomer, E. (2017, November 21). Uber concealed cyberattack that exposed 57 million people's data. Bloomberg. https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data

Etherington, D. (2017, November 21). Uber data breach from 2016 affected 57 million riders and drivers. TechCrunch. https://techcrunch.com/2017/11/21/uber-data-breach-from-2016-affected-57-million-riders-and-drivers/

National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (NIST SP 800-53 Rev. 5). https://doi.org/10.6028/NIST.SP.800-53r5

Uber Technologies, Inc. (2017, November 21). 2016 data security incident (Blog post by D. Khosrowshahi, CEO). Uber Newsroom. https://www.uber.com/newsroom/2016-data-incident/