2-Government Technology-After Uber

Lohrmann on Cybersecurity

After Uber Data Breach: Lessons for All of Us

Another major data breach stunned the world in November, but this incident was unique in several ways. What can we all learn from the Uber data breach? Here's an industry roundup of security analysts' lessons learned from Uber, as well as my top takeaways for all of us.

December 01, 2017 •

Email

credit: shutterstock

What could be worse than a major data breach involving millions of records that occurs at a well-known global company affecting millions of personal records?

Answer: a cover-up of the entire incident *[Deny]*. Add in a payment to hackers to try to have the stolen data deleted, and call those payments a bug bounty . Add in delays in reporting the data breach to the appropriate authorities, and the scope of Uber's troubles becomes scary. *[Anger, Disappointment, Deny]*

What Happened at Uber?

According to The NY Times :

"Uber disclosed Tuesday that hackers had stolen 57 million driver and rider accounts and that the company had kept the data breach secret for more than a year *[Deny]* after paying a $100,000 ransom. …

[Compliance]

The two hackers stole data about the company's riders and drivers — including phone numbers, email addresses and names — from a third-party server and then approached Uber and demanded $100,000 to delete their copy of the data, the employees said.

Uber acquiesced to the demands *[Compliance]*, and then went further. The company tracked down the hackers and pushed them to sign nondisclosure agreements *[Disappointment]*, according to the people familiar with the matter. To further conceal the damage, Uber executives also made it appear as if the payout had been part of a 'bug bounty *[Deny]*' — a common practice among technology companies in which they pay hackers to attack their software to test for soft spots. …"

On Nov. 29, Uber disclosed that 2.7 million people in the UK were affected by the security breach. The Guardian (UK) reported :

Uber has admitted that 2.7 million people in the UK were affected by a 2016 security breach that compromised customers' information, including names, email addresses and mobile phone numbers.

The ride-hailing company had previously disclosed that 57 million people worldwide were affected by a breach that it covered up for more than a year *[Deny]*.

It published an estimate of the number of UK drivers and passengers for the first time, prompting concern from the mayor of London , where Uber is already battling a decision to revoke its license to operate.

What Went Wrong After the Uber Data Breach?

TheOutline.com reported more details of what was going on behind the scenes at Uber with their company leadership.

Clearly [former Uber CSO Joe] Sullivan and [former CEO Travis] Kalanick agreed $100,000 was worth it *[Disappointment, Anger]*, if only to save the company some bad press — Uber was in the middle of negotiating with the

Federal Trade Commission (FTC) for failing to disclose an unrelated data breach in 2014 *[Disappointment]*. This was just one of Sullivan's many ethical breaches at the transportation company, however.

Uber has a documented habit of surveilling people it deems to be a potential threat, including employees, competitors, and its opponents in court. Sullivan was the one to order underlings to dig up dirt on the conservationist Stephen Meyer, who sued Uber for price fixing.

Sullivan operated autonomously and secretly. Sources also told Bloomberg that Sullivan had made himself more nimble by becoming Uber's deputy general counsel, which let him "assert attorney-client privilege on his communications with colleagues and make his e-mails more difficult for a prosecutor to subpoena." Bloomberg wrote in October that "Sullivan's work is largely a mystery to the company's board." *[Worry]*

Sullivan was in charge of a team formerly known as Competitive Intelligence or COIN, according to Bloomberg, which oversaw projects like "Hell," which spied on Lyft drivers. Sullivan shut down Hell but kept other programs like it, and COIN was renamed to "Marketplace Analytics" and then again to "Marketplace Integrity." The 57 million-person hack came to light because Uber's board hired a law firm to investigate Sullivan's teams, including COIN.

On Tuesday, a former Uber employee alleged that Sullivan encouraged his teams to use ephemeral messaging apps in order to "make sure we didn't create a paper trail that would come back to haunt the company in any potential criminal or civil litigation *[Deny]*."

Who Is Suing Uber — and Why?

The list of public-and private-sector organizations that are suing Uber is growing by the day. *[Legal Action]* Dark Reading reported :

"First, on Monday, the city of Chicago and Cook County filed a lawsuit asking the court to fine Uber $10,000 a day *[Legal Action]* for each violation of a consumer's privacy. The suit contends Uber took much too long to report the breach.

Next, on Tuesday, Washington state Attorney General Bob Ferguson filed a consumer protection lawsuit against Uber *[Legal Action]*, asking for penalties of up to $2,000 per violation. The lawsuit alleges that at least 10,888 Uber drivers in Washington were breached, so the lawsuit could result in millions of dollars of penalties.

On top of the two lawsuits from state and local governments, Uber has also been hit with two class-action lawsuits *[Legal Action]*. Both cases were filed last week. The first, Alejandro Flores v. Raiser was filed in federal court in Los Angeles. The second lawsuit, Danyelle Townsend and Ken Tew v. Uber , was filed in federal court in San Francisco. *[Legal Action]*

Multiple state governments also say that they are conducting investigations into the Uber breach *[Legal Action]*. Dark Reading has confirmed ongoing investigations by the states of Connecticut, Massachusetts, Missouri, and New York." *[Legal Action]*

The Seattle Times reported that: "Washington Attorney General Bob Ferguson is suing Uber *[Legal Action]*, after the ride-hailing company waited more than a year to reveal that it had been hacked *[Deny]*, resulting in the breach of personal data for customers and drivers. …

'Washington law is clear, when a data breach puts people at risk, businesses must inform them *[Anger]*,' Ferguson said, in announcing what he billed as a multimillion-dollar lawsuit. 'Uber's conduct has been truly stunning. There is no excuse for keeping this information from consumers *[Anger]*.'

About 50 million Uber passengers had their names, addresses and phone numbers breached, but the hackers also got driver's license numbers for about 7 million Uber drivers, including 10,888 in Washington, Ferguson said.

Industry Lessons Learned: What Can Everyone Learn from This Evolving Uber Case Study?

While these investigations and lawsuits will likely take years to resolve, security industry experts have been quick to offer lessons learned from this

situation. Here are a few of the more notable articles that I have seen on this Uber data breach topic — with the details available at the linked articles:

The first lesson is that the cover-up is always worse than the crime *[Disappointment]*.

The second lesson is that data breaches are no longer a matter of if, but when.

The third lesson is that an independent perspective is essential.

Bottom Line: Companies should establish cybersecurity response procedures and test their plans. These policies and procedures are a helpful framework and starting point, and they serve to raise awareness within the organization that coordination is necessary. But CEOs must avoid the temptation to treat these procedures as security blankets *[Worry]*.

ITPro.co.uk: Uber Hack a lesson in how not to handle a data breach

A ‘simple’ hack strikes again

Uber failed its ‘social responsibility *[Disappointment]*’ — “Organisations like Uber have a social responsibility not only to do their best to protect the data they control, but to be transparent with their users about the risks to their identity, *[Disappointment]*” says Jeremiah Grossman, chief of security strategy at SentinelOne. “How an organisation responds to a breach is what really separates the good from the bad.”

Review the security of your cloud deployments.

Regarding disclosure: Honesty and forthrightness are key.

Your security and your brand are inextricably linked.

Customer Perception Will Impact Your Business.

Security Awareness Is Everyone’s Job.

Prompt Detection and Response Are Critical

Another good set of points comes from the Financial Times (FT.com) in the article: The Uber data breach has implications for all of us.

“But this latest scandal is not just bad for Uber. By handing those in favour of stricter privacy regulation a new stick with which to beat the tech companies, Uber’s behaviour will have a negative impact on all digital service providers *[Disappointment]*. Rightly so, some will argue. The distinction between the Silicon Valley tech companies and traditional industries has become increasingly blurred. …” *[Disappointment]*

My Top 3 Takeaway Lessons for Everyone

Know applicable data breach notification laws in your jurisdiction. Have a plan in place to respond and recover from cyberincidents that ensures compliance with the law.

Don’t Cover Up Data Breaches. The ramifications of a cover-up can be worse than the actual breach. This may seem like an obvious lesson, but the Uber case is full of twists and turns that should serve as warning signs to public-and private-sector executives *[Worry]*. There is no doubt that using the word “incident” makes sense at first, and there are many incidents that are not breaches.

However, this article from law.com suggests that data breach cover-ups may be more common than many people think. “Although there are data breach notification laws on the books in 48 U.S. states requiring companies to inform consumers about potential exposures of their personal information, companies don’t exactly have great incentives to disclose a potential data breach. Disclosing data breaches tends to invite scrutiny from investors, open the door to litigation, and may not play well for a company’s reputation.”

Ensure the appropriate ethical rules and guidelines are well-understood and communicated to all employees , including actions taken surrounding incidents — including senior management. Make sure all necessary employees are engaged in ongoing cybertraining. Also ensure that table-top exercise based are planned regularly, based upon on these policies and procedures.

No company or government is exempt from the ramification of poor ethical behavior. The Uber name and brand reputation are suffering more because of the actions taken after the breach. *[Disappointment]*Well-prepared companies and governments can avoid this extra brand damage.

Final Thoughts

There is little doubt that this Uber data breach is one of the top cybersecurity stories in 2017. No, it doesn't rise to the level of the Equifax data breach, nor does it have nearly the same level of impacts to the global financial system or customers.

Nevertheless, the Uber brand name has already been badly tarnished *[Disappointment]*, and the long-term viability of the company is even being questioned by some *[Disappointment]*. At a minimum, the fallout of this Uber data breach will be felt for years. These developments at such an innovative company are amazing, given that "ubering" has becoming a verb (like googling), which includes dramatically changing a business process using data and digital transformation .

Meanwhile, for the rest of us who are watching events unfold, a key question is whether Uber riders and drivers will lose trust in the company. Other lawsuits were revealed in the past week *[Legal Action]* which allege that Uber used covert tactics to steal rival secrets *[Deny]*.

No doubt, Uber should (and will) get a chance to tell their side to these stories in court, but customer trust is the ultimate key. As Uber plans to build out its "new transportation world" with a future that includes autonomous cars that can pick up and drop off our children virtually anywhere, will we trust them with our data? *[Worry]*

That is the (multi) billion-dollar question. And everyone is watching and taking detailed notes.