4-CSO Online-Uber data breach

Opinion

Uber data breach – an insurance case study for directors and officers

When we evaluate the merits of what actually took place, we will see an interesting scenario develop that could directly impact Uber’s board of directors.

Magdalena Petrova

On November 21, 2017, Uber announced that the personal data of 57 million users were stolen in a breach, including 600,000 drivers in the United States. Reuters just reported that “Uber received an email last year from an anonymous person demanding money in exchange for user data and the message was forwarded to the company’s bug bounty team in what was described as Uber’s routine practice for such solicitations, according to three sources familiar with the matter.”

When we evaluate the merits of what actually took place, we will see an interesting scenario develop that could directly impact Uber’s board of directors. So, let us first examine how this breach compares with others. In Figure 1. We see that the raw number of records disseminated is low when we compare against other major breaches. However, how many of the other breaches exposed both client and employee data?

According to Uber, the demand for money came in and they forwarded the demand to the team that handles bug bounties (a type of contest many large firms employ to help ensure their cyber risk mitigation strategies are up to par by challenging the hacker community to try and identify a weakness that would garner a cash award – in this case up to $10,000).

The first problem with this theory the underwriters need to consider is that this is not how a bug bounty program “should” work. The intent is to identify a material weakness, proven with a proof of concept, and then get

paid. If you take your activities to the next level – and actually "steal" information – not only does that violate the law, it generally null and voids the terms and conditions set forth by the bug bounty program itself. But Uber's program has no such language. Here's what language is present:

Exposure of User Data: the ability to access user or employee data without having an authorized relationship from the Victim.

In-scope vulnerability class examples:

AWS Identity & Access Management credential exposure resulting in access to driver documents in an S3 bucket.

Adding a user to a Partner's account, without them accepting the invite, resulting in exposure of name, phone number, and trip history.

Password reset token exposure, allowing attacker the ability to reset password of victim and login to view sensitive user data.

IDOR/authorization vulnerabilities resulting in exposure of personal data.

Out-of-scope vulnerability class examples:

The ability to determine if a phone number or email has an Uber account, also known as an account oracle.

Potential domains to look at: auth.uber.com, partners.uber.com, riders.uber.com, eats.uber.com

There does not appear to me a scenario either in or out of scope that would be consistent with what Uber alleges took place. The ability to access is not the same thing as "exfiltration." Even if this is the case, the dollar threshold is exceeded by 10x. So, something is not right here. Was this simply a tactic to downplay the event?

Was this a simple oversight by Uber's staff when they received the demand? Was there a corporate policy in place to define what to do in the face of a ransom? Perhaps a subsection of their Incident Response Plan?

If we do some quick math using the infamous IBM and Ponemon statistics, the cost per record is $141.00 each. If we use that metric, we look at over $8 Billion in potential loss. Do I believe that it will cost them this amount, not likely.

Reading " Executive Liability for Data Breach Notification Delay? " by Kevin LaCroix made me think of the potential financial implications to underwriting this cyber event and its linkage with Directors and Officers lines of coverage.

Uber has a fairly new CEO who was not present at the time of the breach as well as a new general counsel, Tony Scott, who was recently quoted as saying:

"I'm not the first to recognize that the company over-indexed on growth without putting in the appropriate guardrails," he said in an interview Friday. "Fostering a culture of compliance is going to be one of my top priorities."

Any company with excessive growth can find it hard to scale in areas that generally go unchecked by most businesses. Such as at what point do I hire a CISO, at what point do I hire additional staff with the following skill sets based on gaps that exist today. Does this constitute willful or intentional wrongdoing, a negating factor for D&O coverage? In my opinion, no. *[Diminish]*

However, what was known by Uber and when? Also failing to abide by 48 State Regulatory Agencies (47 at the time of the breach), becomes the discerning factor (or should be) by the insurance carrier(s).

If Uber submits a claim for damages incurred by the theft of data, are they entitled to do so under a cyber policy? Depends on the following:

Was the policy written in a manner that imposes limits of liability when state laws applicable to data breach notification are not met?

Is a future claim of damages negated if you fail to use the carrier's post-breach service providers?

Was the insurance application constructed in a manner that took into account the use of a third party, in this case GitHub, and what was Uber's inherent obligations to protect sensitive software development?

Did the underwriters, brokers, or agents even assess the bug bounty program for assertion of potential exclusionary provisions?

Now comes the interesting part. Since we are a litigious society and there is always an attorney to champion a good cyber breach case, there exists a chance that Board Members could be subject to being swept into this debacle. Are there factors under a D&O policy that could convert over to negating the cyber policy?

According to Mackoul and Associates there are 10 scenarios that void a D&O claim. I draw your attention to the first line item "Breach of Contract". The reason for this is that a contractual duty is not a liability imposed by law but rather a voluntarily undertaken obligation. Failure to comply with a signed contract would fall under willful or intentional wrongdoing and would not be covered.

There may exist a claim of breaching the contract by the 600,000 employees. If you go to Uber's privacy site , you will see how they define their own policy.

For a number of years, the Federal Trade Commission has levied sanctions against companies for either misrepresenting or not adhering to stated privacy policies on corporate websites as an unfair and deceptive business practice.

While this case is still under investigation and more information is sure to surface, can the mere fact that Uber willfully did not advise each State Attorney General as basis for breaching a contract between employer and employee if the employer had a lawful duty to disclose? If the answer is "yes" then this factor alone could negate any top cover a D&O policy may provide

Furthermore, as described by Mackoul, under the header of "Willful or Intentional Wrongdoing"

“A board may still be able to recover a fine resulting from intentional conduct if it can prove that it was only vicariously liable for misconduct but willful or intentional wrongdoing is normally not covered by D&O policies.”

Was this incident made aware to the board prior to public disclosure? If yes, what actions did they take to ensure State laws were met? If they did nothing and failed to meet the standard of care, does that constitute willful or intentional wrongdoing? Did they even know about these requirements and if not, is ignorance of the law an excuse to vacate a guilty decision from being rendered? Short answer after over 1,000 hours in a courtroom, “no.”

Next read this