Careem
The Data Breach of the First Unicorn in The Middle East

Tareq Haboukh
132105214

Security, Privacy and Ethics for Business Analytics
Dr. Amir Ghazinoori

March 29, 2022.
- 1,200 word -

What started as a typical day at work turned out to be my first real-life experience of working for a company in the aftermath of a security breach, at the time I worked at the Amman Careem office. Leadership team conducted an urgent meeting to discuss the circulating rumors of a possible data leak as they informed us that Careem intends to release a public statement the next day. They prepared us for what potential consequences might be and explained that it was the right thing to do. The breach affected millions of the ride-hailing app's day-to-day users as well as thousands of Captains “Careem drivers” who make a living working on its platform. This event had a significant impact on the company and sparked a change in how the company dealt with security issues and lead to the implementation of major IT infrastructure improvements.

On January 14, 2018. The most notable ride-hailing app from the middle east suffered from a cyberattack that compromised the data of about 14 million app users as well as 558,000 Captains who worked on its platform. The hackers were able to access a computer system used to store information about customers and captains such as their names, email addresses, phone numbers, and trip information. The company announced the breach on Monday, April 23rd. three months after they first learned about the incident and claimed that all users who signed up on the platform after the day of the breach were safe and are not affected. (Paul)

The fast-growing startup operating across 14 countries and 78 cities at the time has issued an apology to its users and sent an email statement to explain the full extent of the incident. They shared information about what happened and how they reacted as soon as they learned about the attack. They assured their commitment to protecting customers' information and that their privacy is a top priority to the company and what they have learned from the experience will help improve network security and make the organization more reluctant to these kinds of cyber threats. while

also advising users on how to implement good password management by updating their Careem account password and any account that might have been compromised, and not to share any personal information or click on links from unfamiliar sources, they also urged users to keep an eye on their banking account and credit cards for any suspicious activities even though there was no evidence that any financial information or passwords were accessed by the hackers because banking data were kept on a third party PCI server that uses international banking security protocols to keep the information safe. (Careem) (Harrison)

As soon as the company was alerted about the data leak, they conducted an internal security investigation and sought out leading cyber security experts to further understand the issue and fortify the security of its network, The company did not comment on the origin of the attack and simply stated they do not know who might have been behind it. The company has implemented various changes to its security infrastructure by establishing monitoring capabilities to identify future attacks and allow them to react faster to security threats. They also implemented multi-factor authentication software to update users' access controls. Careem security team still believed there was room to improve its security and they planned to do so in the upcoming months. (Dawn)

The company knew about the attack for three months but choose not to reveal the news to the public before they were sure they had all the information related to it. and that they do not notify the hackers about their awareness of the breach before fixing the security issues. In contrast, a security expert from Amman criticized the delay and called it completely unacceptable, he argued that the company gave the hackers more time to use the data they acquired while users had no idea their information have been compromised by the breach, many other critics shared this view. (Harrison) The press raised questions about the implications of the leak of trip information (pick up and drop off location) for political figures, activists, and journalists but the company gave little

details claiming they were working closely with the authorities and are unable to disclose such information. (Dawn)

According to Farooq Bloch, the company was warned many times before about its security vulnerabilities by white hat hackers and Pakistani researchers, this goes all the way back to 2016. He claims the breach could have been easily averted if they have fixed the issues highlighted but unfortunately, they did not take any of those warnings into consideration as they fell on deaf ears. There were many attempts to inform the company by white hat hackers over many platforms such as Twitter, email and they reached out to people from sales, marketing, engineering to the extent of meeting with a country head "Junaid Iqbal", but with all the effort it seemed like the company was not interested. Ethical hackers simply did not want the vulnerabilities to be exploited by malicious groups that can do actual harm to the users and the company itself. (Baloch)

In 2016 a bounty hunter was able to identify a security flaw and gained access to information about customers and Captains. The information included live car locations and other critical details. This should have been a red flag to the company, but Farooq explained that technology startups usually in their early phases tend to focus on short-term gains and overlook the long-term security aspect of the business. A $100,000 in bounty hunting programs would have resulted in better security and let the company take advantage of the collective efforts while keeping the information of their users secure, instead, they relied only on their internal security team to fix those bugs. (Baloch)

Uber Technologies, once rival and now the owner of Careem Networks suffered from the same type of attack in October 2016, the hackers were able to obtain the data of 57 million customers and drivers. The data included the name, email addresses, phone numbers of 50 million users, and personal information of 7 million drivers. The incident resulted in Uber paying the attackers $100,000. (Dawn)

In my opinion, Careem gambled with the privacy of their customers in the company's early stages by making poor security decisions that lead to the breach. they have prioritized fast-paced growth over everything else and suffered the consequences and paid a hefty price. Fortunately, they have learned their lesson and since the attack, they have taken the responsibility for their actions and shifted their IT strategy to ensure top-notch security. I also think that the public appreciated the heartfelt transparency from the company which is something people are not used to experience in the region, to be frank. Careem has taken major steps in improving security especially now that they have joined forces with Uber. Of course, there is more to be done as threats become more and more sophisticated. But overall, I believe they are on the right track. Going back to this old memory and reading in-depth about what happened opened my eyes to the notion of how easy it is to overlook information security even when you have all the best intentions.

References

Baloch, Farooq. *Who is to blame for Careem's criminal data breach?* 28 4 2018. 25 3 2022. <https://profit.pakistantoday.com.pk/2018/04/25/did-careem-pay-for-its-ignorance/>.

Careem. *Important Careem Security Information*. 4 23 2018. 25 3 2022. <https://blog.careem.com/en/security/>.

Dawn. *Careem users' personal data compromised in massive data breach*. 23 4 2018. 25 3 2022. <https://www.dawn.com/news/1403401>.

Harrison, Peter. *Hackers access personal data of 14 million Careem taxi users*. 23 4 2018. 25 3 2022. <https://www.arabnews.com/node/1289791/business-economy>.

Paul, Katie. *Dubai's Careem hit by cyber attack affecting 14 million users*. 23 4 2018. 3 25 2022. <https://www.reuters.com/article/us-careem-cyberattack-idUSKBN1HU1WJ>.