Treyton Davis

CS-405

June 7, 2024

Module Five Case Study

**Introduction**

The data breach case I am going to go through is the January 2023 T-Mobile data breach. This breach made the news due to 37 million customers being affected by this breach. T-Mobile notified the Securities and Exchange Commission on January 5, 2023 about a bad actor(s) accessing parts of their systems. The link to the report is: [T-Mobile January 2023 Breach (sec.gov)](https://www.sec.gov/ix?doc=/Archives/edgar/data/0001283699/000119312523010949/d641142d8k.htm).

**Description of Breach**

The data breach happened due to a bad actor(s) accessing the data of 37 million T-Mobile customers through a single Application Programming Interface (API). The API did not allow the bad actor(s) to access personal data (payment methods, social security numbers, government IDs, or PIN/passwords), however the API did allow access to customer names, billing addresses, email addresses, phone numbers, date of birth, T-Mobile Account Numbers, number of lines on the account, and plan features.

The reason T-Mobile has been a larger target of attack versus Verizon and AT&T is that T-Mobile did not always have their systems secured to protect customer data. After the 2021 breach, T-Mobile signed a multi-year investment to be working with external cybersecurity experts to help improve cybersecurity capabilities and transform how their cybersecurity approach works.

**Threat Identification**

The immediate threat that was shown was that T-Mobile never locked down the API with authentication measures to ensure no outside user would have access to that information. Another threat would have been T-Mobile losing customers since 37 million users would have hurt T-Mobile and made all their efforts to improve security pointless if there are no customers to protect.

One potential threat that could’ve happened if the vulnerability was unresolved would be that the same bad actor(s) or new actor(s) could’ve accessed the same API to try and harvest more information from the servers to try and release info on all T-Mobile customers plus all of the Mobile Virtual Network Operators (MVNOs) that operate on T-Mobile’s network, causing more than 200 million users have personal data stolen.

**Breach Prevention**

T-Mobile and their developers could’ve prevented this breach by ensuring all APIs required authorization to access anything to prevent any outside actor(s) from accessing the systems. They have fixed this by consulting with cybersecurity experts to trace the source and stop the breach. The systems and policies that were already in place helped prevent the loss of sensitive customer data (social security numbers, card information, and government IDs).

**Summarization of Best Practices**

T-Mobile had an API that did not require authorization or authentication, allowing for a bad actor(s) to access and steal information of 37 million postpaid and prepaid customers. Had there been an authentication and authorization layer, it would have prevented such a large number of customers losing personal information.