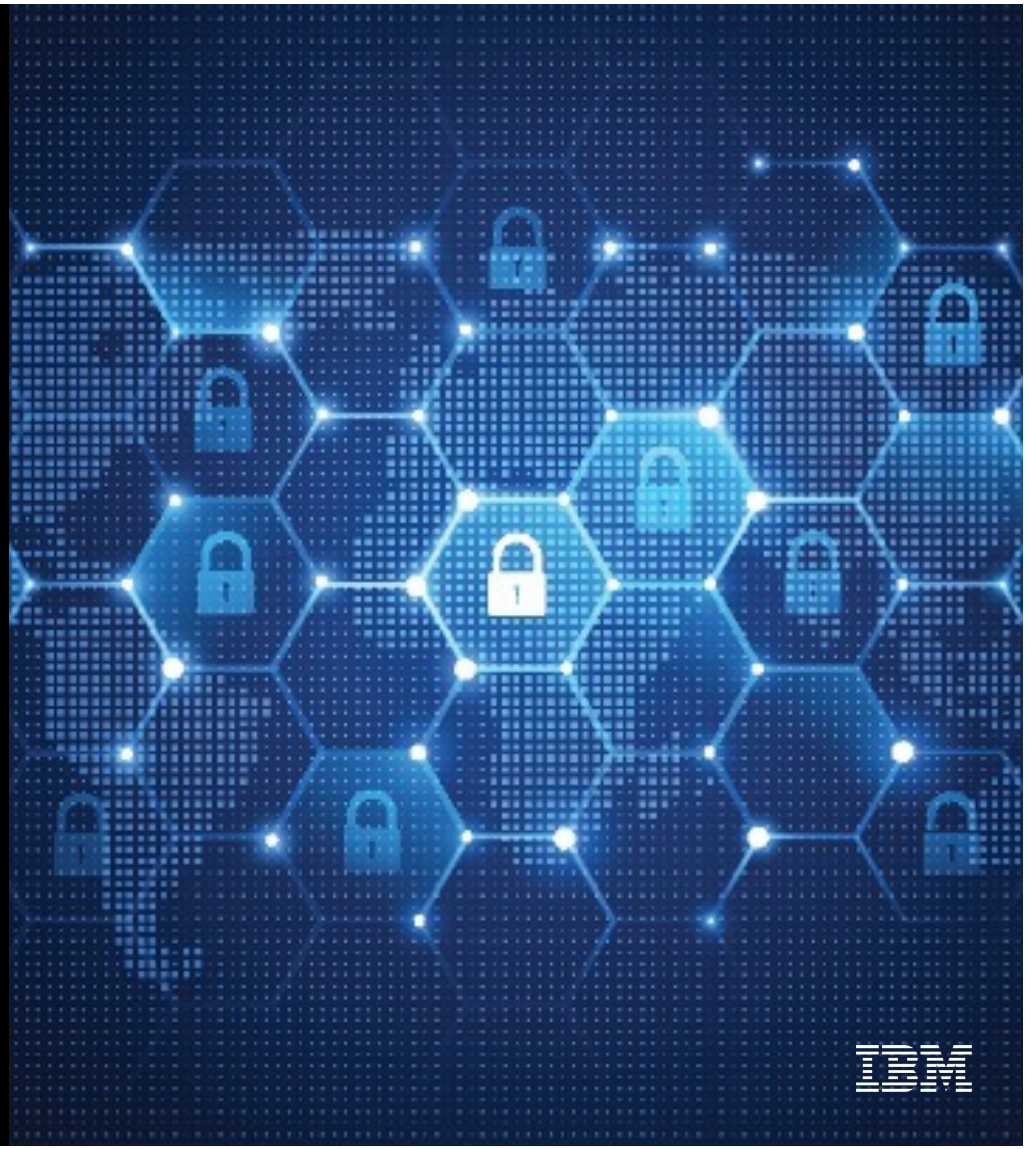
Case Study

Supply Chain Attack

AT&T / Data Leak



Attack Category:
Supply Chain Attack

Description of the Attack Category:
The AT&T data breach is an example of a **third-party vendor attack** or **supply chain attack**. In this type of attack, cybercriminals target a third-party vendor that has access to a company's data or systems.
The attackers exploit vulnerabilities in the vendor's security to gain unauthorized access to the company's data.
In the case of AT&T, the data breach involved sensitive customer data, including names, account numbers, phone numbers, and email addresses. The data was then leaked on the dark web.

Statistics about this Type of Attack:
Data breaches are a significant issue in the telecommunications industry. A report from cyber intelligence firm **Cyble** estimates that more than 74 million U.S. telecom customers had their data leaked on the dark web in 2023. In terms of cost, as of 2023, the average data breach cost across businesses worldwide was 4.45 million U.S. dollars.
Each leaked data record cost about 165 U.S. dollars. The United States saw the highest average breach cost globally, at 9.48 million U.S. dollars.

Sources:

1. AT&T Confirms Third-Party Data Breach Exposing 9 Million Customer Accounts
2. AT&T data breach hits nine million customer accounts
3. AT&T 70M User ‘Data Breach’: Expert Analysis
4. AT&T, T-Mobile and other telecom data breaches highlight industry's weaknesses
5. Data records breached worldwide Q4 2023

Company Description and Breach Summary

AT&T Company Description:

AT&T Inc. is a leading provider of telecommunications, media, and technology services globally. The company offers wireless communications, data/broadband and internet services, local and long-distance telephone services, telecommunications equipment, managed networking, and wholesale services.

AT&T's integrated network of 5G and fiber has you covered. As of 2024, AT&T was ranked 13th on the Fortune 500 rankings of the largest United States corporations, with revenues of $120.7 billion.

AT&T Breach Summary:

AT&T has acknowledged a data breach dating back to 2021. Personal data belonging to 73 million current or former AT&T customers has been leaked online.

Information including addresses, social security numbers, and passcodes was published on the dark web. The data involved in the breach appears to be from 2019 or earlier and is linked to 7.6 million customers and 65.4 million former account holders. It also includes information such as full names, email addresses, and dates of birth.

AT&T said financial information had not appeared in the leak. The company has reset customers' passcodes and recommended fraud alerts from credit bureaus.

Timeline

AT&T Data Breaches: Full Timeline Through 2024

1. **November 25, 2022:** A bad actor started obtaining data through a single Application Programming Interface (API)
2. **March 2023:** AT&T notified 9 million customers that their data had been exposed following an attack on a third-party vendor2
3. **October 2023:** There have been no reported AT&T data breaches since the incident in March
4. **March 19, 2024:** An archive allegedly containing information on 73 million AT&T customers leaked on the open internet.
5. **March 30, 2024:** AT&T announced that it had reset the passcodes of 7.6 million customers after it determined that compromised customer data was released on the dark web
6. **March 31, 2024:** AT&T began notifying customers whose personal information was compromised

Vulnerabilities

The AT&T data breach involved vendor security vulnerabilities, passcode compromise, uncertainty of data origin, and exposure of personal information, leading to potential risks of financial fraud and identity theft for customers.

Vulnerability 1

Vendor Security Vulnerabilities

In a previous breach in January 2023, hackers targeted one of AT&T's marketing vendors rather than the company itself.

The attackers exploited one of the vendor's security vulnerabilities, which has since been patched

Source

Vulnerability 2

Passcode Compromise

AT&T admitted that a number of passcodes have been compromised.

Unlike passwords, passcodes are numerical PINs that are typically four digits long

Source

Vulnerability 3

Data Origin Uncertainty

AT&T stated that it doesn't know if the massive data breach "originated from AT&T or one of its vendors," indicating a potential lack of visibility or control over data security.

Source

Vulnerability 4

Personal Information Exposure

The breached data included sensitive personal information such as Social Security numbers, names, dates of birth, and possibly addresses.

This presents customers with a new set of risks, including financial fraud and identity theft.

Source

Costs and Prevention

According to the 2023 Cost of a Data Breach Report by IBM and the Ponemon Institute, the global average cost of a data breach was USD 4.45 million

Costs

- Financial Impact:
  The exact financial cost of the breach to AT&T is not publicly disclosed. However, such breaches often result in significant costs related to customer notification, legal fees, regulatory fines, and enhanced security measures.
- Reputation Damage:
  Data breaches can significantly damage a company's reputation, leading to loss of customer trust and potentially decreased
- Stock Impact:
  The AT&T share price may have been affected by the data breach.
- Customer Impact:
  The breach affected approximately 7.6 million current and 65.4 million former customers, potentially leading to identity theft and other forms of fraud.
- Legal Consequences:
  AT&T could face legal consequences, including lawsuits and fines, due to the breach.

Prevention

- Change Passwords:
  Customers should change their passwords associated with all AT&T accounts.
- Beware of Phishing Attacks:
  Since AT&T has not confirmed that data has come from them, customers should be very aware of phishing and social engineering attacks that claim to be from AT&T addressing or offering services to protect you from the data leak.
- Freeze Credit/Set Up Identity Monitoring:
  Customers should consider freezing their credit and/or setting up identity monitoring.
- Monitor Accounts:
  Customers should monitor their accounts for any suspicious activity.
- Regularly Update Software and Systems:
  AT&T and its customers should ensure that all their software and systems are regularly updated to protect against known vulnerabilities.