National Forensic Sciences University

School of Cyber security and Digital Forensics

Subject: CTMSCS S2 P4 Incident Response and Digital Forensics

(TA-II Assignment)

Submitted to: Mr. Ramya Shah and Mr. Nilay Mistry

Submitted by: Disha Sharma (240103002014)

Submission Date: 15/04/2025

INDEX

INTRODUCTION

The personal genomics firm 23andMe experienced a data breach that was publicized in October 2023. Millions of users' profiles and ethnicity data were collected by the cyberattack. According to reports, the impacted individuals included hundreds of thousands of ethnically Chinese users in addition to the majority of Ashkenazi Jews. Name, profile photo, birth year, location, family surnames, grandparents' birthplaces, ethnicity estimates, mitochondrial DNA haplogroup, Y-chromosome DNA haplogroup, link to an external family tree, and any text content a customer had optionally included in their "About" section were among the details the hacker or hackers took from customers that they had chosen to share with their DNA matches. The business acknowledged on October 6, 2023, that the hacker or hackers had illegally obtained information belonging to roughly 6.9 million users.

A hacker going under the name Golem claimed to have taken over millions of individuals' 23andMe profiles in October 2023. According to the firm, the incident was caused by hacking techniques such as "credential stuffing," which allowed unauthorized access to millions of customers' profile information. Privacy concerns were raised by the compromised data, which contained user profile personal information.

The guardian rightly quotes the motivation for this attack:

“Three years ago, a man in Florida named JL decided, on a whim, to send a tube of his spit to the genetic testing site 23andMe in exchange for an ancestry report. JL, like

millions of other 23andMe participants before him, says he was often asked about his ethnicity and craved a deeper insight into his identity. He said he was surprised by the diversity of his test results, which showed he had some Ashkenazi Jewish heritage.”

BACKGROUND

A sample of data points from 23andMe accounts were made public on BreachForums, a community dedicated to black-hat hacking crimes, according to an article published by Wired in October 2023.

23andMe told TechCrunch that the actual number of people exposed was 6.9 million, or almost half of the 14 million customers that 23andMe stated, due to an opt-in function that permits DNA-related relatives to get in touch with one another.

A hacking community raised worries about targeted assaults after promoting one set of data as a list of Ashkenazi Jews and another as a list of people of Chinese origin. Only after a user commented about the up-for-sale data on a 23andMe subreddit in early October did 23andMe openly admit the hackers' attacks. According to an inquiry into the incident, since at least April 2023, hackers had been attempting—and occasionally succeeding—to obtain access. By the end of September, the attacks had lasted for over five months. According to a 23andMe representative who emailed the Guardian, the business did not "detect a breach" within its systems and instead blamed the situation on hacked recycled login credentials from certain customers.

ATTACK VECTORS

1. Credential Stuffing

The incident was a credential-stuffing attack in which usernames and passwords used for the 23andMe website were the same credentials used for other websites, from which they were stolen.

The compromised information varies from user to user but includes ancestry and health information. The threat actor also accessed user files related to 23andMe's DNA Relatives feature and proceeded to post this information online.

23andMe is now giving affected individuals notification that the threat actor's activity has been contained. Additionally, it adopted a two-step authentication login process for its website and mandates that users reset their passwords.

The company has been the target of several class action lawsuits, and in its third fiscal quarter, it anticipates spending between $1 million and $2 million on costs associated with the breach.

ATTACK SURFACE

1. User Accounts

Because user accounts frequently contain access credentials and sensitive personal data, they constitute a crucial component of the attack surface. User accounts can be targeted by attackers using:

Credential stuffing is the practice of gaining unauthorized access by using credentials that have been stolen from earlier breaches.
Phishing is the practice of tricking someone into divulging their login credentials by using phony emails or websites.
Weak Passwords: Taking advantage of accounts that have readily guessed or frequently used passwords on various platforms.

Organizations can reduce these risks by enforcing strong password standards, implementing multifactor authentication, and training people to spot phishing attacks.

2. API Endpoints

API endpoints are interfaces that facilitate communication between various software programs. They are essential for exchanging data, however if not adequately secured, they may be attacked:

Injection Attacks: Malicious code, such as SQL injection or cross-site scripting (XSS), can be injected by attackers using inadequately secured APIs.
Unauthorized Access: Unauthorized users may gain access to APIs that do not have adequate authorization and authentication checks.
Data Exposure: If APIs are not set up properly, they may unintentionally reveal private information.

Implementing strong authentication procedures, verifying input data, and routinely checking API security setups are all necessary to secure API endpoints.

3. Data Storage Systems

Large volumes of sensitive data are stored on data storage systems, which makes them an ideal target for hackers:

Data breaches: Sensitive and personal information may be exposed as a result of unauthorized access to storage systems.
Attackers may use ransomware to encrypt data and then demand a ransom to unlock it.
Insider threats are the potential for contractors or employees who have access to data storage systems to abuse that access for malevolent ends.

Organizations should employ encryption, put access controls in place, and carry out frequent security audits to find and fix weaknesses in data storage systems.

Organizations can better prepare and execute strategies to reduce potential cybersecurity threats by comprehending these attack surface components.

ARCHITECTURE TARGETED

1. Cloud Data Storage

23andMe securely manages and stores enormous volumes of genetic data via cloud data storage. Important factors in this architecture are as follows:

Scalability: As more people submit their genetic data, the cloud infrastructure needs to be able to manage massive data volumes.

Security: To safeguard sensitive genetic data, data encryption is essential, both in transit and at rest. Regular security audits and access controls aid in preventing unwanted access.

Compliance: The storage system must to abide by laws like the U.S.'s Health Insurance Portability and Accountability Act (HIPAA), which regulates the security and privacy of medical records.

2. User Authentication Systems

To guarantee that only individuals with permission can access their genetic data, user authentication is essential. This includes the following with relation to 23andMe:

Multifactor authentication (MFA): By asking users to submit additional verification, such as a code texted to their mobile device, MFA adds an extra layer of security on top of a login and password.

Strong Password Policies: To prevent unwanted access to user accounts, it is helpful to promote or enforce the usage of strong, one-of-a-kind passwords.

Session management: In order to prevent unwanted access, user sessions are secured and inactive sessions are ended after a predetermined amount of inactivity.

3. API Architecture

The 23andMe platform's many components may communicate and offer services to consumers thanks to APIs. Among the crucial elements of API architecture are:

Using secure tokens or keys, authentication and authorization make sure that only authorized people or systems can access APIs.

Strict input validation should be put in place to guard against injection attempts and guarantee that the API processes only legitimate data.

Rate Limiting and Throttling: Preventing abuse of APIs by restricting the quantity of requests that a system or user may submit in a specific amount of time.

IMPACT OF THE BREACH

Using a straightforward saliva test, 23andMe, which was once valued at $6 billion, gave customers access to genetic information about their ancestry and health. It contained one of the biggest private DNA databases in the world, with more than 15 million users. However, the business experienced a significant data breach in 2023 that compromised 6.9 million accounts. This has led to the exposure of a wealth of private and sensitive genetic data.

In March 2025, the business is now declaring bankruptcy. The company is aggressively looking for a buyer, and co-founder Anne Wojcicki has resigned as CEO amid the financial difficulties.

Naturally, the announcement of bankruptcy is significant. What will happen to all of the consumer DNA data that 23andme has, however, is a much more significant story. In the event that the business is acquired, what will happen to the genetic profiles? To whom will they be available? In what circumstances? To what extent, if at all, is this data protected?

These are not only hypothetical inquiries. Rather, they serve as a wake-up call for both people and companies.

There is an implicit trust relationship when customers give a business their data. Data is not the only thing compromised in a breach. The trust pact is shattered into a thousand fragments.

The core values of 23andMe's brand were empowerment and scientific curiosity. However, consumers started to doubt that promise's very basis after the hack. Such harm to one's reputation is frequently lethal.

Breach costs money. The average cost of a breach was $4.88 million, per IBM's 2024 Cost of a Data Breach Report. It was the start of the end for 23andMe. Revenue decreased and customer trust declined. The company's value plummeted from billions to less than $50 million by 2025.

MITIGATION STRATEGIES

Advanced filtering is used by email security companies to stop viruses, phishing attempts, and spam before they ever reach an employee's inbox. They lower the possibility of human error by continuously screening emails for questionable payloads, links, and behavioral patterns. Unfortunately, breaches are mostly caused by people.

We require assistance in order to train clients in cybersecurity awareness, assist teams in identifying warning signs, and steer clear of dangerous behaviors because the human element is such a significant weakness. Your first line of defense should be a knowledgeable team.

The takeaways from 23andMe for company owners are clear:

- By design, privacy is required.
- Email security needs to be completely secure.
- Openness fosters trust.
- A breach response plan is necessary.

REFERENCES

- *Encyclopædia Britannica*, Encyclopædia Britannica, inc., www.britannica.com/chatbot. Accessed 15 Apr. 2025.

- “Hackers Got Nearly 7 Million People’s Data from 23andMe. the Firm Blamed Users in ‘very Dumb’ Move.” *The Guardian*, Guardian News and Media, 15 Feb. 2024, www.theguardian.com/technology/2024/feb/15/23andme-hack-data-genetic-data-selling-response.

- “23andMe Data Leak.” *Wikipedia*, Wikimedia Foundation, 10 Dec. 2024, en.wikipedia.org/wiki/23andMe_data_leak.

- “Understanding the 23andme Data Breach and Ensuring Cybersecurity.” *Risk Strategies - Insurance Brokerage & Consulting Firm*, www.risk-strategies.com/blog/understanding-the-23andme-data-breach-and-ensuring-cybersecurity. Accessed 15 Apr. 2025.

- *23andMe: Data Breach Was a Credential-Stuffing Attack*, www.darkreading.com/cyberattacks-data-breaches/23andme-files-credential-stuffing-attack-with-sec. Accessed 15 Apr. 2025.