About the Course Project

Introduction

Welcome to the final project of the Cybersecurity Capstone course. This final project is a culmination of the course, preparing you to make an immediate impact in the field.

In this project, you will apply case study analysis and reporting skills to research, analyze, and propose recommendations for a real-world data breach.

The project, which comprises three tasks, will take about 90 minutes to complete.

Task 1

Identify a suitable, real-world cybersecurity case study that provides valuable insights for analysis.

The selected case study should be relevant to cybersecurity topics, such as:

- Cyberthreats and cyberattacks
- Networking and network security
- Database security
- Application security
- Artificial intelligence (AI)
- Governance, risk, and compliance
- Penetration testing
- Threat hunting
- Encryption
- Cybersecurity architecture
- Incident response
- Digital forensics
- Cryptography

You will then write a clear and concise introduction to the case study in a maximum of 150 words.

Task 2

Provide two credible citations that reference the case study you selected.

Task 3

Use the standard case study analysis template to document your observations. This template has been used throughout the course for each case study.

In this template, you will cover the following sections:

- Root cause
- Actions taken
- Evaluate effectiveness and timeliness
- Successes, gaps, and failures
- Impact on the organization
- Lessons learned
- Recommendations for future actions
- Conclusion

Ensure to read the prompts carefully and provide suitable responses.

Once you've completed the project, submit it for AI evaluation.

Introduction to the Final Project: Analyzing a Data Breach

Welcome to this video that introduces you to the final project, Analyzing a Data Breach. After watching this video, you will be able to

- effectively analyze a case study using the case study analysis template explained in this course.
- You will also be able to identify a suitable case study.

Case Study Evaluation

At the beginning of this course, you are provided with recommendations for conducting a case study evaluation. The same case study analysis template was used throughout the course to work through each case study. Additionally, throughout the lessons, you completed activities that guided you through each section of the analysis template. In this final project, you will have to identify a case study to evaluate.

You'll then use the provided template to analyze the case study.

Template Sections

Let's review each section of the case study analysis template.

- In the **Root Cause section**, you will identify the initial point of failure, breach, or necessity for change. You'll analyze the factors contributing to the vulnerability or need for action.
- In the **Actions Taken section**, you'll list all the steps and measures taken to respond to the incident or facilitate the change. Be sure to include details such as dates, personnel involved, and the resources used.
- In the **Evaluate Effectiveness and Timeliness section**, you'll assess how effective and timely the actions were in solving the incident or implementing the change. You have to support your evaluation with metrics or feedback.
- Then, in the **Successes, Gaps, and Failures section**, you'll pinpoint the successes achieved, gaps identified, and failures encountered during the response or change process. Providing specific examples will enhance clarity.
- In the **Impact on the Organization section**, you'll discuss how the successes, gaps, and failures you identified may affect the organization in the short and long term, considering operational and strategic implications.
- Next, in the **Lessons Learned section**, you'll summarize the key lessons learned from the incident or change process, highlighting positive takeaways and areas for improvement.
- In the **Recommendations for Future Actions section**, you'll provide clear recommendations on what actions should be taken and what actions should be avoided in future incidents or change processes. These recommendations should be actionable and based on the lessons learned.
- **Conclusion**: Finally, you'll reflect on the broader implications of the case study for the organization and the industry. Ensure to highlight any trends or patterns that emerged and their potential long-term effects. You should have at least two references for your research.

Tips to find a suitable case study

Here are some tips to help you find a suitable case study.

- **Focus on relevance**. Look for case studies on cybersecurity topics. These could include networking security, database security, application security, encryption, AI, compliance, pen testing, threat hunting, cybersecurity architecture, incident response, or digital forensics.

- **Consider the scope** of the case study. Look for case studies that provide enough detail to analyze the successes, gaps, failures, and impact on the organization.
- **Seek credible sources**. Look for case studies from reputable sources such as academic journals, industry publications, reputable news sources, or other trusted organizations.
- **Use real-world examples**. Your chosen case study should involve real-world situations and scenarios. These studies will offer practical insights and lessons learned from actual experiences.

In this video, you learned that

- the case study analysis template includes the following sections – Root Cause, Actions Taken, Evaluate Effectiveness and Timeliness, Successes, Gaps, and Failures, Impact on the Organization, Lessons Learned, Recommendations for Future Actions, and Conclusion.
- You also learned that when looking for a suitable case study, it is important to focus on relevance, consider the scope, seek credible sources, and include real-world examples.

Case Study Analysis: 23andMe Data Leak (2023)

Cybersecurity Capstone Final Project

Natascha Martin

August 30, 2025

Task 1: Introduction

The 23andMe data leak of 2023 highlighted serious risks in the protection of personal and genetic information. Attackers used a credential-stuffing attack, relying on previously leaked passwords from breaches. This worked because many users reused the same passwords across different platforms, and 23andMe did not require multifactor authentication to block unauthorized access. As a result, nearly 3.9 million profiles were compromised, including data about users' ethnicity and DNA relative connections.

While the company pointed out that its core systems were not directly breached, the exposure of sensitive genetic data created privacy, ethical, and regulatory concerns. This incident also damaged customer trust, since this information cannot be changed like a password or credit card number.

This case study is important because it shows how common cyber attacks like credential stuffing can have serious consequences when combined with weak security controls, and highlights the need for stronger protections in the genetics industry.

Root Cause:

The primary cause of the 23andMe data leak was a credential-stuffing, in which a hacker known as "Golem", reused passwords from previously exposed breaches to gain access to user accounts (Holthouse, Owens, & Bhunia, 2025). This attack was effective because many users recycled old credentials across multiple platforms.

A second critical factor was the lack of enforced multifactor authentication (MFA), which left accounts vulnerable once passwords were compromised. Without mandatory MFA, attackers only needed a valid email and password to successfully log in, making the breach scalable and damaging (Information Commissioner's Office, 2025).

Actions Taken:

After the breach, 23andMe required users to reset their passwords and advised them to create stronger, unique ones. The company also rolled out MFA, but only as an option, not a requirement. These measures added a layer of protection for the future, but they came after millions of accounts were already exposed, making the response feel late (23andMe, 2023).

Effectiveness & Timeliness:

The response was limited because it happened after the attack had already succeeded. Resetting passwords and adding optional MFA helped reduce the risk of future issues but did nothing for the data already taken.

Since MFA was not enforced, many accounts were still vulnerable. Overall, the company's actions showed the need for stronger, proactive monitoring instead of waiting until after the damage was done (Holthouse et al., 2025).

Success, Gaps, and Failures:

One success was that “Golem” never got into the 23andMe’s core databases, which mean the company’s infrastructure was not fully breached. But there were clear gaps in security: many customers reused old passwords, and 23andMe did not require MFA to protect against that. A major failure was in poor communication, since the company was slow to admit how widespread the breach really was, leaving customers uncertain for too long (ICO, 2025).

Impact on the Organization:

The data leak damaged customer trust and hurt 23andMe’s reputation, especially since genetic information is more sensitive than regular personal data. Customers and regulators questioned whether the company could keep this type of data safe. On top of reputational harm, 23andMe faced lawsuits and fines, which increased the financial and legal consequences of the breach (ICO, 2025).

Lessons learned:

The breach showed how dangerous credential stuffing attacks can be, especially when people reuse passwords across different platforms. It also highlighted that companies handling extremely sensitive information, like genetic data, need stricter protections than standard consumer accounts. Enforcing MFA and detecting unusual activity earlier could have reduced the impact of the attack (Holthouse et al., 2025).

Recommendations:

23andMe should make MFA mandatory for all users, not just optional. The company also needs stronger monitoring and anomaly detection systems to spot large scale login attempts before they escalate. These improvements would reduce the chance of future breaches and help rebuild customer confidence (23andMe, 2023).

Conclusions:

The 23andMe breach highlights the risk of weak authentication and the dangers of relying only on passwords. It shows why governance, compliance, and honest communication with customers are essential when handling highly sensitive personal data. By enforcing stronger authentication and improving its response strategy, 23andMe can reduce risks and better protect its users going forward (ICO, 2025).

Task 2: Sources:

23andMe. (2023, October 6). *Addressing data security concerns – Action plan.* 23andMe Blog. https://blog.23andme.com/articles/addressing-data-security-concerns

Information Commissioner's Office. (2025, June 17). *23andMe fined £2.31 million for failing to protect UK user's genetic data* [New release]. ICO. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/06/23andme-fined-for-failing-to-protect-uk-users-genetic-data/

Holthouse, R., Owens, S., & Bhunia, S. (2025, February 6). *The 23andMe data breach: Analyzing credential stuffing attacks, security vulnerabilities, and mitigation strategies* [Preprint]. arXiv. https://arxiv.org/abs/2502.04303