CSC 4585/5585: Software and Systems Security

Case Study Reporting On A Recent Data Breach

This case study report is a group activity where either 3 or 4 students will group together to submit the final data breach analysis report (Groups are already created in iLearn, you should be able to see who works with you in this activity). You will pick a recent (happened in between 2023 to 2025) data breach incident either in United States or in Europe. I am providing some recommended list if you want to choose any of these events.

Data Breach Incidents: [You can also pick from outside of this list as long as it is within the given time and location restrictive, mention your selected data breach clearly in the executive summary]

- **MOVEit Data Breaches (2023)**
- **3CX Supply Chain Attack (2023)**
- **Trello Data Breach (2024)**
- **Microsoft Cloud Email Breach (2023)**
- **Capita plc Data Breach (2023)**
- **Consumer Financial Protection Bureau (CFPB) Breach (2023)**
- **National Public Data Breach (2024)**
- **Change Healthcare Breach (2024)**
- **Snowflake Inc. (cloud-data platform) (2024)**
- **Allianz Life Insurance Company of North America (2025)**

Now, once you have selected a data breach, you should have the following information regarding the incident in your report. [Note: Please write your own report and not AI generated ones]

The report will have the following items:

Group ID: #

Group Members: <list of student names>

1. Executive Summary

- Briefly summarize the breach, including what happened, when it was discovered, and the main affected areas. This section should give an overview without delving into too many technical specifics but should highlight the breach's significance.

2. Incident Details

- **Date and Time of the Incident**: Record when the breach was initially detected and any known dates of unauthorized access.

- **Description of the Breach**: Include what type of data was accessed (e.g., personal, financial, health data) and how the breach occurred (e.g., phishing, malware, system vulnerability).
- **Affected Systems and Data**: Identify which systems were impacted and specify the types of data compromised.

3. Root Cause Analysis

- Describe the cause of the breach (e.g., a misconfigured server, phishing attack, ransomware attach, or software vulnerability). Students should analyze how the attacker was able to exploit these weaknesses, emphasizing any technical failures, policy gaps, or human errors. Please provide necessary references or links as citations to acknowledge the source of the information.

4. Breach Detection and Response Timeline

- Provide a timeline of events (i.e., use a timeline chart/figure), from detection through response stages. This includes when the breach was identified, when mitigation efforts started, and any updates made to stakeholders. This helps illustrate incident response effectiveness and response times.

5. Impact Assessment

- **Affected Parties**: Describe the impact on customers, employees, or third-party affiliates. Specify the number of people/customers or organizations affected.
- **Data Sensitivity and Potential Harm**: Highlight the potential harm to affected individuals, such as risk of identity theft, financial loss, or privacy invasion.
- **Financial and Operational Impact**: If relevant, estimate any financial damage (e.g., lost revenue, recovery costs) and operational disruptions caused by the breach.

6. Notification and Communication

- Describe the steps taken to notify affected individuals, regulatory authorities, and, if relevant, the media. Students should mention the content of these notifications and any measures offered to those impacted (e.g., identity theft protection).

7. Mitigation and Remediation Efforts

- Outline what actions were taken immediately to contain the breach and any longer-term security measures put in place to prevent similar incidents. This might include software updates, network segmentation, revised access controls, or employee training on phishing awareness.

8. Recommendations for Future Prevention

- Based on the incident's root cause, list recommendations for improving security posture. This may include implementing stronger access controls, conducting regular security audits, or enhancing endpoint security.

9. Legal and Compliance Considerations

- Address any legal implications, such as compliance with data protection laws (e.g., GDPR, CCPA) and regulatory penalties. Mention any potential consequences the organization might face and how they plan to address compliance issues moving forward.

10. Conclusion

- Summarize the main findings and emphasize lessons learned. Highlight the importance of cybersecurity and proactive measures in preventing future incidents.

11. References

- All the references are added in standard technical report format

Submission items:

[Note: You need to submit ratings of all the team members based on their timely participation and efforts in group activity/discussion while completing the case study. It is essential to understand that you are not making any technical evaluation but rather identify if someone is a team player or not]

- **Item-1:** PDF report with the above items **[75%]**
- **Item-2:** 5-7 minutes Video Presentation of your report/case study **[25%]** [Note: Going over 8 minutes or below 5 minutes may impact the grading]
- **Item-3:** Ratings of group members. Example if given below: (ratings can be fractional as well)

Members	**Ratings (out of 10)**
Ron	10, 9, 10 **(Ron's rating will be given by Jhon, Mills, and Casey here…Ron will not provide rating for himself)**
Jhon	9, 8, 10 **(Jhon's rating will be given by Ron, Mills, and Casey here…Jhon will not provide rating for himself)**
Mills	10, 10, 10
Casey	7, 7, 8