THE STATE UNIVERSITY OF ZANZIBAR

SCHOOL OF COMPUTING COMMUNICATION AND MEDIA

DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

GROUP ASSIGMENT

SN	STUDENT NAME	REGISTRATION NUMBER
1.	AISHA ABDALLA SALUM	BITAM/10/22/061/TY
2.	UMMUL-KULTHUM HAMAD SULEIMAN	BITAM/10/22/019/TZ
3.	YUSFIA YUSSUF ALI	BITAM/10/22/042/TZ
4.	ZUHURA MAULID YUSSUF	BITAM/10/22/022/TZ
5.	RAMADHAN BABU CHIRIKU	BITAM/10/22/045/TZ

COURSE CODE: INF 3202

COURSE TITTLE: IS STRATEGY AND AQUSITION

COURSE INSTRUCTURE: DR. MARIAM

ASSIGNMENT: SECURITY BREACHES ANALYSIS

SUBMISSION DATE: 30/06/2025

INTRODUCTION

Security breach means when someone enters computer systems, networks, or gets private information without permission. This happens mostly because of weak security, mistakes, or old systems.

1. Equifax Breach (2017)

What Happened:

A group of hackers found a weak point in Equifax's system software called Apache Struts. Using this, they accessed personal details of around **147 million people** in the USA. They stole Social Security numbers, birthdates, home addresses, some driving license numbers, and credit card details of **209,000 people**.

Effects:

- It was one of the biggest cyber-attacks in history.
- People stopped trusting the company.
- Many personal documents were taken by attackers.
-

What We Learn:

- Always update and fix system software on time.
- Companies should protect sensitive information better.
- They should test and improve their security plans often.
- Private data needs strong protection at all levels.

2. Capital One Breach (2019)

What Happened:

A former employee of Amazon Web Services found a mistake in Capital One's cloud security settings. The person used that mistake to steal over **100 million records**, including bank details, credit information, and Social Security numbers.

Effects:

- The company lost a lot of money.
- They faced legal cases.
- Many people doubted the safety of cloud services.

What We Learn:

- Cloud security settings should be checked regularly.
- Monitor employees' activities to avoid inside attacks.
- Inside workers can also cause big security problems.

3. Microsoft Exchange Attack (2021)

What Happened:

Hackers discovered four new weaknesses in Microsoft Exchange Servers used for emails. These allowed them to break into systems without needing passwords. They gained control of emails and company networks. Many businesses and government offices were affected.

Effects:

- Different attackers used the weakness.
- Some victims faced more attacks like ransomware.
- IT teams spent a lot of time fixing the problem.

What We Learn:

- New system weaknesses should be fixed immediately.
- Using cloud-based services can reduce the chance of attacks.
- Strong network controls help limit damage.
- Detecting strange activities early helps to respond fast.

4. Facebook Data Exposure (2021)
What Happened:
A problem in Facebook's contact feature allowed attackers to collect user information. Over **530 million accounts** were affected. Details like names, phone numbers, locations, and emails were leaked.

Effects:

- Personal details were exposed online.
- Scam and phishing risks increased.
- Facebook was criticized for weak data protection.

What We Learn:

- Online platforms must prevent data scraping.
- Inform users quickly when data leaks happen.

5. Marriott Hotels Breach (2018)
What Happened:
Hackers entered the Starwood hotel system, which Marriott had bought. They accessed data of about **500 million guests** over several years. Information included passports, credit card numbers, and personal contact details.

Effects:

- Travelers' personal details were stolen worldwide.
- Marriott faced fines and lawsuits.
- Their name and trust were damaged.

What We Learn:

- Check security when buying other businesses.
- Use encryption to protect personal data.
- Improve ways to detect and stop attackers.

CONCLUSION
These examples show that weak systems, old software, or human mistakes can lead to big security problems. Companies must always improve their protection, update systems, train their staff, and take data privacy seriously to avoid cyber-attacks.

References

1. https://www.bbc.com/news/technology-56662281
2. https://www.csoonline.com/article/3531087/the-capital-one-data-breach-everything-you-need-to-know.html
3. https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security.html
4. https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-settles-ftc-equifax-breach
5. https://www.marriott.com/about/newsroom/2018/marriott-announces-starwood-guest-reservation-database-security-incident.
6. U.S. Federal Trade Commission Reports
7. Wired, TechCrunch, BBC Cybersecurity Articles
8. Official Company Breach Statements
9. Cybersecurity & Infrastructure Security Agency (CISA)