Yahoo Data Breach (2013–2014) – Summary Report

Prepared by: Judy Raj

Overview

In 2013 and 2014, Yahoo experienced two major data breaches that affected a total of 3.5 billion accounts. The attacks exposed names, email addresses, phone numbers, birth dates, and hashed passwords. The breaches, undisclosed until 2016, represent the largest known cybersecurity incident in history.

Root Causes

- Weak encryption (MD5) and outdated security practices.
- Poor vulnerability management and delayed detection.
- Exploited cookie-generation code that enabled unauthorized access.

Actions Taken

Yahoo strengthened encryption standards, invalidated unencrypted security questions, and appointed a Chief Information Security Officer to oversee security reforms.

Organizational Impact

- $35M SEC fine for delayed disclosure.
- Significant stock decline and shareholder lawsuits.
- Severe erosion of customer trust and reputation.

Lessons & Recommendations

Adopt strong encryption (e.g., AES-256), enforce multi-factor authentication, and establish proactive breach detection with timely disclosure protocols. Embed cybersecurity governance into enterprise culture.

Conclusion

The Yahoo breaches underscore the need for vigilance, transparency, and continuous improvement in cybersecurity. Effective data protection requires proactive risk management and strong governance at all organizational levels.

References

StrongDM, Dark Reading, SEC Press Release (2018), Reuters, and Wired.