Submitted by: Ankit Pradhan

Course: IT Security: Ethical and Legal Issues

Section: A

Date: October 1, 2025

Professor: Ionut Anghelache

Company: Twitter/X (now X Corp.)

## INTRODUCTION

Twitter, rebranded as X, is a major social media platform used worldwide for public discourse, business communication, and information sharing. Headquartered in San Francisco, Twitter/X serves hundreds of millions of users daily and is influential in social media ecosystems globally. Its large user base and vast troves of personal data make it a high-value target for cybercriminals. [1]

This report analyzes the January 2023 data breach at Twitter/X, one of the largest social media breaches in recent years affecting millions of users. The incident demonstrates critical cybersecurity challenges faced by large platforms handling sensitive user information and the extensive impacts such breaches can have. [2], [3]

## SUMMARY OF THE INCIDENT

The Twitter/X data breach traces back to a vulnerability initially discovered in January 2022 within Twitter's Application Programming Interface (API). This flaw enabled attackers to correlate email addresses and phone numbers with Twitter account information such as usernames and profile details. Though Twitter/X patched the flaw after it was disclosed through its bug bounty program, attackers exploited this bug to scrape data from millions of accounts before the fix was fully effective. [4], [5]

By late 2022, a dataset containing approximately 400 million Twitter/X accounts appeared for sale on dark web forums, although experts noted many duplicate entries. Analysts later confirmed that around 200 million records from this dataset were authentic. This dataset included sensitive information like email addresses, user IDs, follower counts, locations, and profile metadata, but no passwords or financial data. [5], [6], [4]

In January 2023, the verified dataset was publicly leaked on hacker forums, further disseminating the user information. In early 2025, a disgruntled insider posted an even larger combined dataset on a major hacking forum, Breach Forums, that merged the 2023 data with a newer breach consisting of over 2.8 billion user profile records, believed to be compiled from scraped data and old accounts. The leaked data comprised user screen names, email addresses, location details, and follower counts, offering ample opportunities for cybercriminals to conduct phishing, identity theft, and social engineering attacks. [1], [2]

Twitter/X publicly acknowledged the initial data incidents but downplayed their severity by stating much of the data was publicly available or compiled from prior leaks. However, cybersecurity experts warned that the addition of email addresses linked with account profiles considerably raised the threat level for users. [6], [4], [5]

## IMPACT(S) ON THE ORGANIZATION

The breach had profound ramifications for Twitter/X:

- **Reputational Damage:** The incident severely damaged Twitter/X's credibility and user trust, raising concerns about the platform's capability to safeguard user information [3], [1]
- **Financial and Legal Risks:** While direct financial data was not compromised, Twitter/X faced potential legal challenges under global privacy legislation, including lawsuits and government investigations for failing to protect consumer data adequately. [2]
- **Operational Strain:** The company was forced to invest heavily in cybersecurity improvements, incident response, and user education programs to combat fallout from the breach. [5]

- **User Security Risks:** Millions of users became vulnerable to enhanced phishing and identity theft attempts due to leaking personal information such as emails and location data. [4]
- **Industry-wide Implications:** The breach exposed systemic weaknesses in social media data security, prompting industry-wide calls for enhanced regulatory compliance and cybersecurity protocols. [3]

## CONCLUSION

The Twitter/X January 2023 breach serves as a stark reminder of the persistent vulnerabilities major technology platforms face in protecting user data. The exploitation of an API vulnerability followed by multiple data repackaging illustrates how minor weaknesses can have magnified consequences over time [6], [4]

For organizations, this incident underscores the crucial need for immediate vulnerability mitigation, transparent breach disclosures, and continuous cybersecurity enhancements. Equally important is educating users about risks and protective measures to minimize long-term harm [1], [2]

Ultimately, this breach highlights that maintaining data security in today's interconnected environment is an ongoing challenge requiring vigilance, innovation, and accountability across all levels of an organization [3], [5]

REFERENCES


[1] PhishingTackle.com, "X (Twitter) Insider Data Breach Exposes Billions Of Profiles," 6 April 2025. [Online]. Available: https://phishingtackle.com/blog/x-twitter-insider-data-breach-exposes-billions-of-profiles.

[2] CyberPress.org, "Massive 400GB of X (Twitter) User Records Allegedly Leaked," 30 March 2025. [Online]. Available: https://cyberpress.org/massive-twitter-data-breach/.

[3] PurpleSec.us, "Data Of More Than 200 Million Twitter Users Is Leaked," 23 July 2025. [Online]. Available: https://purplesec.us/breach-report/twitter-data-leak-200-million-users/.

[4] FirewallTimes.com, "Twitter Data Breaches: Full Timeline Through 2023," 4 October 2023. [Online]. Available: https://firewalltimes.com/twitter-data-breach-timeline/.

[5] HaveIBeenPwned.com, "Twitter (200M) Data Breach," 4 January 2023. [Online]. Available: https://haveibeenpwned.com/breach/twitter200m.

[6] GRCReport.com, "Diving into the X Data Breach: Over 200 Million User Records Exposed," 8 April 2025. [Online]. Available: https://www.grcreport.com/post/diving-into-the-x-data-breach-over-200-million-user-records-exposed.