Risk Assessment Report

Name: Victor Obiora

Cybersecurity

10/11/23

1 Introduction

The purpose of this report is to present the findings of a risk assessment exercise carried out from June 2021 to January 2022 with the scope described below. The main purpose of the exercise was to assess the risks to Twitter and to identify which of these could be accepted and which may need some action to be taken to address them.

Once this risk assessment report has been approved, specific actions will be identified, discussed, agreed and then documented in a risk treatment plan to be managed as part of the Information Security Management System (ISMS).

The process used for this risk assessment is set out in the document Risk Assessment and Treatment Process which is part of the ISMS.

This risk assessment report describes:

- The context and scope of the risk assessment
- The assets within scope
- Threats to, and vulnerabilities of, those assets

This report is input to the risk treatment stage of the process and must be signed off by top management before continuing further.

This risk assessment was carried out by the following people:

NAME	ROLE IN ASSESSMENT
Victor Obiora	Lead risk assessor

Table 1: Risk assessment team

As part of the assessment, the following additional people were consulted:

NAME	TITLE	LOCATION
Parag Agrawal	Chief Technology Officer	California office
Cathleen Pacini	HR Manager	California office

Table 2: People consulted

2 Risk assessment context

This section describes the reasons why the risk assessment was carried out, the areas that were within its scope and the criteria that were applied in order to decide which risks are recommended for acceptance.

2.1 Internal and external context

[Explain the reasons why the risk assessment was carried out and the potential benefits from it.]

The reason why the assessment was carried out was to identify the vulnerabilities within the organization's systems and processes, which in this case is the Twitter's API. From there they would assess the impact to understand the severity of the incident by knowing what data was compromised and the number of users that were affected, to reinforce compliance with the standards and regulations, prevent future incidents, and to protect the organization's reputation.

The potential benefits for carrying out risk assessment include:

- Risk Mitigation
- Data Protection
- Regulatory Compliance
- Reputation Management

2.2 Scope

[Set out the boundaries of the risk assessment in terms of what it does and doesn't cover.]

For example:

This assessment addresses the risks to cloud service customers' personally identifiable information held within [Organization Name] multi-tenanted systems in order to ensure that we comply with recent changes in legislation in this area. It does not cover risks to other types of data such as company financial information and intellectual property. Personal data held within the systems of other companies within the group is also not covered.

This assessment addresses the risks by identifying the specific vulnerability in the Twitter API that was exploited, gauging the impact of the breach, the detailed time-line of the events, the security measures that were put in place before the breach, and how effective it was in preventing the breach, and finally, the evaluation of Twitter's compliance with data

protection and privacy regulations, as well as any potential legal implications and consequences.

3 Risk assessment results summary

A summary of the outcome of the risk assessment is shown in Table 3.1 below.

[Identify the top two assets from your table and explain what they are and why you prioritized them. Also, elaborate on the threat and the impact they will have to the company if lost/stolen/damaged/etc.]

The two assets chosen are **User Data** and **Twitter API**.

User data

The threat involves unauthorized access, data theft, identity theft, and potentially fraudulent activities using stolen user information. The impact of the data breach can lead to reputational damage, loss of trust, legal consequences, and potential financial losses due to user attrition.

Twitter API

The threat here is that malicious actors can exploit the vulnerability to access user data and potentially perform unauthorized actions on the platform. If not addressed promptly, this vulnerability could lead to recurring data breaches, legal and regulatory repercussions, and damage to Twitter's reputation.

3.1 ASSET-BASED ASSESSMENT

[Complete the table below as thoroughly as possible for your organisation by thinking of as many of the assets as possible. Classify them by Type as either (P)hysical - computers for example, (F)unctional - a company process for example, or (S)ocial - the company reputation for example. Pick two of these assets and determine the threat to this asset. Speculate on what would happen if it was damaged or lost in the Additional Comments]

REF	ASSET	TYPE (P/F/S)	THREAT	ADDITIONAL COMMENTS
1	User data	S	Unauthorized access and exposure.	If user data is damaged or lost, it could result in a breach of user privacy, identity theft, and damage to the company's reputation.
2	Twitter API	F	Exploitation of vulnerabilities.	in the Twitter API can lead to unauthorized access and data breaches
3	Brand reputation	S	Negative publicity and loss of trust.	A damaged reputation may result in the decrease in user engagement, loss of advertisers, and a decrease in the company's stock value. Rebuilding trust can be a long and challenging process.
4	Data security measures	F	Weaknesses or exploitation.	Damage to security measures can expose the platform to further vulnerabilities and breaches. This could lead to more data breaches and reputational damage, eroding trust in the platform's ability to protect user data.
5	User trust	S	Decrease user trust and engagement.	If the user engagement is significantly impacted due to the breach or compromised security, Twitter may face decreased user activity, lower user growth, and a loss of advertisers and revenue.

Table 3: Risk assessment results summary (asset-based)

Figure 1: Asset-based risk assessment

Risk Assessment Matrix

Assets

User data

Risk 1 – a data breach can erode user trust in the platform and potentially lead to decreased user engagement and loss of revenue.

Risk 2 – Violating data protection regulations mat result in significant fines.

Risk 3 – Twitter may face lawsuits from affected users for failing to protect their data.

Twitter API

Risk 1 – Unauthorized access to user data

Risk 2 – Failure to secure the API can lead to Twitter's reputation and trust in its services.

Risk 3 – a compromised Twitter API can lead to hijacking if attackers gain access to user credentials, email addresses, and phone numbers.

Likelihood

1 – Highly unlikely
2 – Unlikely
3 – Possible
4 – Likely
5 – Highly Likely

Impact

1 - Minimal
2 - Minor
3 - Moderate
4 - Major
5 - Catastrophic

Assets	Risk 1	Risk 2	Risk 3	Average
User data	4 x 3 = 12	3 x 1 = 3	4 x 4 = 16	31/3 = 10.33
Twitter API	5x 4 = 20	4 x 2 = 8	5 x 5 = 25	53/3 = 17.67