
EQUIFAX

1 Introduction

The purpose of this report is to present the findings of a risk assessment exercise carried out from 10/10/23 to 17/10/23 with the scope described below. The main purpose of the exercise was to assess the risks to Equifax 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
Kole Reece	Lead risk assessor

Table 1: Risk assessment team

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

NAME	TITLE	LOCATION
Mark Begor	Chief Executive Officer	Chicago office
Sunil Bindal	EVP and Chief Development Officer	London 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

The risk assessment was carried out to catalogue the company's assets and to help the executive team understand and prioritize the risk to each asset. This will help the company to develop policies to guide their cyber security response and improve overall cyber security posture. The risk assessment will help to reduce the likely hood of a cyber attack and reduce the severity of a successful attack. It will also help to ensure compliance with legal requirements. In addition, the assessment will result in reduced cost because the cost of a cyber attack can be significant in terms of financial losses. A cybersecurity assessment can help organizations to avoid these costs by identifying and mitigating security risks.

2.2 Scope

This document assesses the risk to customer data and the infrastructure that both stores and allows customers to access the data It does not investigate the risks to the company's reputation or its human assets. It also does not cover the risk to the company's financial assets.

Likelihood scale

Likelihood	Value
HIGHLY UNLIKELY	*1*
UNLIKELY	*2*
POSSIBLE	*3*
LIKELY	*4*
HIGLY LIKELY	*5*

Impact Scale

Likelihood	Value
MINIMAL	*1*
MINOR	*2*
MODERATE	*3*
MAJOR	*4*
CATOSRPHIC	*5*

Risk assessment matrix

Asset	*Risk1 (Likelihood*Impact)*	*Risk 2 (Likelihood*Impact*	*Risk 3 (Likelihood*Impact*	*Average*
Customer Data	4 * 5=20	*3 * 4 =12*	*3 *5 = 15*	*15*
Network	*3 * 4 = 12*	*4 * 4 = 16*	*3 * 4 = 12*	*13*
Database Server	*3 * 4 = 12*	*3 * 4 = 12*	*4*3=12*	*12*
Website/Webserver	*3 * 3 = 9*	*3 * 5 =15*	*4 *3=12*	*12*
Software systems	*3 *3=9*	*3*4 =12*	*3*4=12*	*11*

3 Risk assessment results summary

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

The top two assets from the table are the Customer data and the company's network. Equifax is one of the three largest credit rating agencies in the United States. Customer data is critical to their business any breach which results in lost stolen or damaged data would be catastrophic for the company. In addition to customer data itself the availability of the data is also imperative to their business. Customers need to be able to access their information for credit checks when required. Any disruption to credit check services because of network outage or DDOS attack would be detrimental to the company. From the risk assessment matrix the Customer Data and Network assets have the highest average calculated risks.

3.1 ASSET-BASED ASSESSMENT

REF	ASSET	TYPE (P/F/S)	THREAT	ADDITIONAL COMMENTS
1	Customer Data	Informational	• Data Could be stolen by malicious actors • Data Could be corrupted. • Insider Threats	If sensitive company data were lost or stolen it could result in significant financial harm to both the company and its customer. An employee could steal and sell customer data
2	Network	Physical	• DDOS attack • Network Compromise • Other Network Outage	Network compromise could lead to the lost of sensitive information including customer data DDOS attack could leave customers unable to access their data
3	Database Server	Physical	• Data could be corrupted. • Date could be stolen. • Hardware failure	Misconfiguration by the database administrator could cause data to be corrupted. SQL injection attack could result in data being stolen
4	Web Server/Website	Physical	• DDOS • Website Compromise • Website Downtime	Website can be hit with DDOS attack. Security vulnerabilities Can leave website open to attack
5	Software Systems	Informational	• Software Systems could contain bugs • Performance problems • Security Vulnerabilities	Bugs in software and security vulnerabilities can have an effect on the availability of customer data

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