CS 6239

Enterprise Cyber Security Management

Case Study 1

1 Company

This case study uses Lyft as an example to analyze threat objectives.

Lyft, Inc., founded in 2012 is a Russell 1000 Index and Nasdaq Index public company providing on-demand MaaS(Mobility as a Service) to 600 million rides a year in United States and Canada.

This case study analyzes the main six threat objects' inherent likelihood and impact of Lyft.

	inherent likelihood	**inherent impact**
DT	possible	severe
EX	probable	high
SA	unlikely	high
FF	probable	high
RH	unlikely	low
WH	unlikely	high

Table 1: Likelihood and Impact for Threat Objectives

2 Threat Objective: Data Disclosure

Inherent likelihood: Possible
Inherent likelihood: Severe

Reason:

Lyft provides high volumes of rides for consumers, and the users' sensitive personal and financial data are the mission critical applications and valuable intellectual property. For example, users' ride history, bank account, payment transaction, home address could be revealed by data breaching or by insider trading.

Once data disclosure happened, the inherent impact would be severe. As a result of data disclosure, costumer tend to lose trust to Lyft, and there could be legal issues and stock price decrease. All of the consequences would harm Lyft's business and reputation.

Although Lyft uses procedures for employees to use VPN and multi-factor authentication (MFA) to access internal application[3], due to the high profit and volume of illegal data disclosure by cyber-criminals and internal threats, the inherent likelihood would be possible.

3 Threat Objective: Extortion

Inherent likelihood: Probable
Inherent likelihood: High

Reason:

The inherent likelihood is probable. There is recent example for large ransomware attack in Lyft, and DDos attacks happen very common in technology companies. In 2022, it was discovered that malicious packages targeting big tech company including Lyft in npm.

When extortion happens, business operations of Lyft would be interrupted or heavily interfered. Especially the data blackmail that threat Lyft's production database or ransomware that disturbs Lyft's on-demand travel planning, which would stop business or even internal platform. If Lyft choose not to pay for ransomware, the pause of business would elongate. Else the comprise price would be high, and negatively influence the revenue.

4 Threat Objective: Sabotage

Inherent likelihood: Possible
Inherent likelihood: High

Reason:

Lyft's physical and cyber infrastructure are possible to be threatened. Since Lyft is a big tech company, the security of physical company facilities is solid, the chance for criminals to physically sabotage the equipment, for example, data center, is unlikely. However, the virtual infrastructure had the history to be hacked. Lyft's industry competitor, Uber Technology Inc. experienced a computer network sabotage in 2022[2]. Therefore, inherent likelihood of sabotage is possible.

When sabotage happened, the impact would be high. Physical and cyber infrastructure are critical to business operation, and disruption would lead to financial losses and extra man hours for fixation.

5 Threat Objective: Fraud

Inherent likelihood: Probable
Inherent likelihood: High

Reason:

Inherent likelihood is probable to happen. Lyft servers over 1 million rides in one day, leading to large transaction and large amount of riders and drivers. Compared to other internet company, Lyft provide mobility as a service, so fraud could happen in car-related activities. For example, riders could fraud by fake report driver's behavior, or driver intercept payment and get their personal information.

Inherent impact is low to serve depending on fraud level depending on fraud severity and fraud scope. Impacts include customer's dissatisfaction, account compromise, and financial loss. The overall inherent impact would be high.

6 Threat Objective: Resource Hijacking

Inherent likelihood: Unlikely
Inherent Impact: Low

Reason:

It's unlikely for Lyft to be attacked by resource hijacking. Criminals could target Lyft's cloud infrastructures for computational resources to mine crypto, or use commoditized malware to access drivers' and riders' personal information. Considering Lyft has a modern and robust vulnerability management system[1], resource hijacking is likely to be detected and reported automatically once begins.

Comparing to other threat objectives, the inherent impact is low. Resource hijacking usually is known by customers, so the business loss and customers satisfaction would not be heavily impacted. Cloud infrastructure repair, maintenance, electrical and memory cost are the main impact.

7 Threat Objective: Watering Hole

Inherent likelihood: Unlikely
Inherent Impact: Low

Reason:

Due Lyft security awareness and the information security practices, watering hole threat is unlikely to happen. However, once zero-day watering hole attack occurs, watering hole attack would not be easily blacklisted, resulting to a high impact. For example, from ride-share business operation to autonomic vehicle test would be contiguously impacted for a relatively long time.

8 Discussion

In this case study of threat objectives of Lyft, we conclude that the data disclosure, extortion, and fraud are top three threats likely to happen, and data disclosure has the severest impact on business.

Therefore, attention should be paid in data disclosure, extortion, and fraud in Lyft's cyber security strategy.

To prioritize the above objectives, Lyft is suggested to closely monitor data breach threat intelligence and news in technology and transportation industry, especially its business competitors(Eg., Uber, Doordash) and giant transportation companies (Eg., UPS, FedEx).

Additionally, Lyft should keep its vulnerability management system updated and recruit experienced talents as DevSecOps Engineer, and Software Engineers for Mobile and Back-end Security.

9 Hypothetical Business

A hypothetical business change Lyft could undergo is using autonomic vehicle to delivery food, which is similar to "Waymo" as "UberEats". This business implies data disclosure threat objectives, since the production data pipeline and machine learning algorithm would be more complicated due to addition of autonomic driving. If Lyft choose third-party vendors for autonomic driving, extortion would possibly occur.

References

[1] Alex Chantavy. Vulnerability management at lyft: Enforcing the cascade - part 1. *Lyft Engineering*, November 2022.

[2] Kate Conger and Kevin Roose. Uber investigating breach of its computer systems. *The New York Times*, September 2022.

[3] Mike Johnson. Lyft: Duo case study. *CISCO Duo*.