Prepared By: Gopi Gor

Date: 01/30/2024

Quick Summary

The two cyber-attacks covered were carried out against MGM and Caesars, two hospitality and entertainment organizations. On September 7, 2023, malicious actors gained access to MGM's network by posing as IT administrators, gaining access credentials to MGM systems. Subsequently, the attackers locked the company's network, preventing resort guests from using electronic room cards, wifi services, ATMs, and related resort services. (SWOT Table 1)

In the case of Caesars Entertainment, similar assets such as reservations, bookings, and casino operations were compromised. This attack was also a result of social engineering, and Caesars reported the hackers gained access to customer information, including driver's license information and SSNs of people signed up with Caesar's loyalty program. However, Caesars did not experience public service outages stemming from the attack. (SWOT Table 2)

S – STRENGTHS	**W – WEAKNESSES**
• They reported to the SEC and didn't pay the attackers.	• MGM has a loss of trust in users and customers.
O – OPPORTUNITIES	**T – THREATS**
• Gave them a chance to implement higher level end-point and domain security. • Credit freeze and credit alerts to be set up.	• In 2019, there was another breach which released 10.6 million users' data, which could have been used for 2023 attack. • Due to the nature of the customer, due to PII, easy target.

S – STRENGTHS	**W – WEAKNESSES**
• They responded really quickly.	• They outsourced the IT for this attack.
O – OPPORTUNITIES	**T – THREATS**
• The quick response and filing to SEC allowed them to save a lot of money in terms of charges they could be involved with.	• They were prone to being attacked again and being asked for a ransom again. • A chance of fraud and identity threat after this. • Due to the nature of the customer, due to PII, easy target.