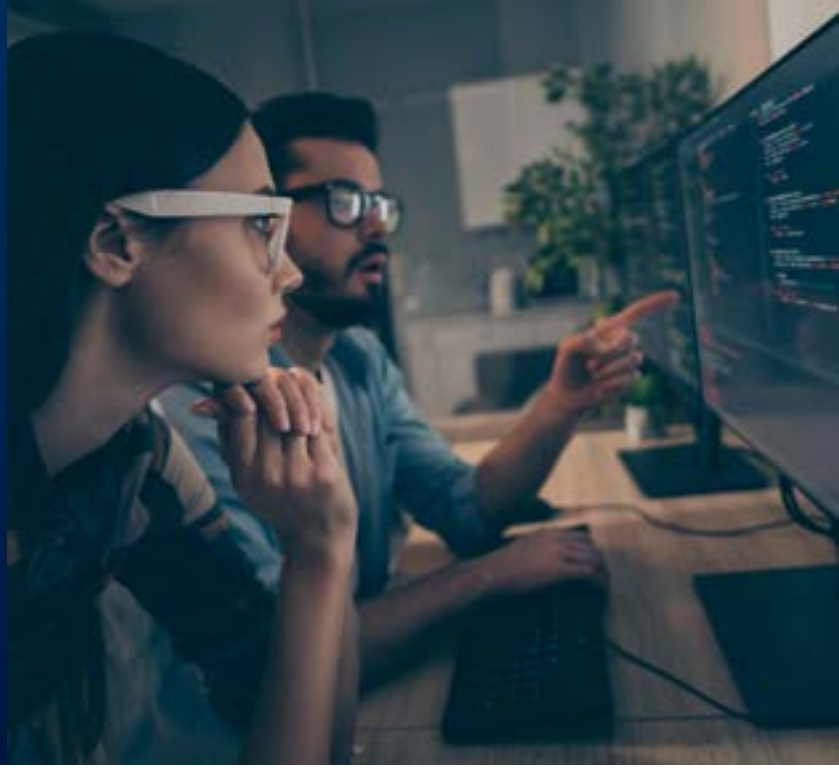
Brown & Brown



PROPERTY & CASUALTY

A Look Back at the MGM and Caesars Incident

The MGM Resorts International and Caesars Entertainment cyberattacks in September 2023 serve as a cautionary tale for those in the cyber world.

Incident Timeline:

- **Early September 2023:** Both MGM and Caesars experience suspicious activity within their IT systems.
- **September 7th:** Caesars suffers a data breach, acknowledging a social engineering attack targeting a third-party IT vendor.
- **September 11th:** MGM faces a ransomware attack by the Scattered Spider (UNC3944) group, causing widespread disruption.
- **September 14th:** Scattered Spider claims to have exfiltrated 6 terabytes of data from both companies.
- **Mid-September:** Caesars reportedly pays a $15 million ransom, while MGM opts for collaboration with law enforcement.
- **Late September:** Both companies restore normal operations.

The attack unfolded in stages. Scattered Spider, a cybercrime group, initially gained a foothold through social engineering, likely phishing for employee credentials. This breach provided access to the Okta platform, a crucial access management system. The attackers then capitalized on weak multi-factor authentication (MFA) to escalate privileges and gain control of the Azure Active Directory domain controller. This unfettered access allowed them to exfiltrate sensitive data and deploy BlackCat/ALPHV ransomware, crippling critical MGM's systems.

The MGM and Caesars attacks were not directly linked but rather showcased the general cyber threats faced by businesses in the hospitality sector. If you imagine two houses on the same street being robbed one after the other, while not directly connected, the incidents highlight a vulnerability in the neighborhood and prompt residents

to improve their security measures. Some reports suggest the same threat actor group (Scattered Spider) might have been involved in both attacks; however, concrete evidence is limited.

Several security shortcomings exacerbated the situation. Inadequate MFA practices, exemplified by the compromised two-factor authentication, proved insufficient to prevent further intrusion. Additionally, a lack of proper security awareness training left employees susceptible to social engineering tactics. Furthermore, the absence of network segmentation granted the attackers unrestricted movement within the system, facilitating lateral movement and data exfiltration. Lastly, limited detection and response (D&R) capabilities delayed the identification and containment of the attack and allowed the situation to escalate.

Learning from these missteps, organizations can take proactive measures to bolster their defenses. Implementing robust MFA solutions with hardware tokens or biometrics significantly strengthens the login process. Regular security awareness training equips employees to recognize and resist phishing attempts. Network segmentation restricts an attacker's reach by isolating critical systems. Investing in advanced D&R tools and processes allows for swifter threat detection and response, minimizing damage. Penetration testing and vulnerability assessments regularly identify and address security gaps before they can be exploited.

The MGM and Caesars incidents serve as a stark reminder of the evolving cyber threat landscape. By adopting a multi-layered approach to cybersecurity, organizations can significantly enhance their defenses. Additionally, an organizaton can improve their recovery process by taking charge of cybersecurity defenses, empowering teammates and employing a team of cyber insurance risk advisors.

How Brown & Brown Can Help

Connect with our Brown & Brown team to learn about our knowledge in your industry, how we build our risk mitigation strategies and how we can aid your business in building a cost-saving program.

Brown & Brown

Find Your Solution at BBrown.com