A Costly Lesson: The 2023 MGM Resorts Cyberattack

The 2023 cyberattack on MGM Resorts is a stark reminder of the vulnerabilities within even the most established companies. While details remain unclear, the attack appears to be a ransomware incident, where attackers likely used social engineering to access MGM's systems. This essay analyzes the nature of the attack, explores how it might have unfolded, and highlights measures that could have prevented it.

Although the reports referenced don't explicitly confirm a ransomware attack, the widespread disruption of services like ATMs and online booking aligns with this tactic. MGM's silence on ransom demands and media reports also suggest such a request may have been made.

The reports hint at a social engineering attack as the initial entry point. Social engineering involves manipulating individuals to gain access to information and implying a vulnerability in either MGM's employee training or IT security protocols. Hackers might have impersonated someone with legitimate access, tricking an employee into revealing login credentials or altering security settings. This compromised access would have allowed them to infiltrate MGM's systems further.

Several security measures could have potentially prevented this attack. Comprehensive training on social engineering tactics can equip employees to identify and avoid such scams. Implementing multi-factor authentication (MFA) adds an extra layer of security, requiring a second verification step even if attackers obtain a login credential. Enforcing strong password policies, including complex passwords and regular changes, reduces the risk of stolen credentials granting access. Finally, regular security audits are crucial in identifying and addressing vulnerabilities in IT systems before attackers exploit them.

By implementing these measures, MGM could have significantly reduced the risk and impact of the attack. The financial cost of the attack was estimated at $100 million, not to mention the potential damage to customer trust. The MGM incident is a valuable lesson for all organizations, highlighting the importance of robust cybersecurity measures and employee training to combat evolving cyber threats.