Case Study: MGM Resorts Cyberattack A Social Science Analysis

Student Name: Gavin Bacaoan

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Professor Diwakar Yalpi

Date: 5 May 2026

Introduction

The 2023 MGM Resorts cyberattack demonstrates how cybersecurity failures often begin with human systems, not just computer systems. In September 2023, MGM shut down parts of its hotel and casino network after a cyberattack disrupted reservations, digital room keys, slot machines, ATMs, and payment services. Customer personal information was also stolen, and the incident was expected to cost the company about $100 million (Page, 2023). The attack has been linked in public reporting to Scattered Spider, a group known for targeting large companies and IT help desks through social engineering (Cybersecurity and Infrastructure Security Agency [CISA], 2023).

Analysis

Technologically, the incident involved identity and access weaknesses. Scattered Spider commonly uses phone calls, SMS messages, SIM swapping, MFA fatigue, and help-desk impersonation to gain credentials or convince staff to reset access controls (CISA, 2023). Social Science explains why these tactics are effective. From psychology, attackers exploit trust,

urgency, fear of disappointing a coworker, and obedience to perceived authority. From sociology, the attack reveals how workplace culture can create risk, and help desk employees may be rewarded for speed and service, while security refusal can feel like a poor customer experience. Anthropology adds another insight: modern workers publicly share job titles, locations, and professional relationships online, making impersonation easier. The societal impact went beyond MGM's internal systems. Guests lost access to basic services, employees faced operational stress, and customers became vulnerable to identity theft. The case shows that cyberattacks can disrupt physical spaces, public trust, labor routines, and privacy.

Solutions

Effective prevention should combine technical controls with social science insights. MGM-like organizations should require phishing-resistant MFA, strict identity verification for password resets, callback procedures, and approval for high-risk account changes. They should also segment hotel, casino, payment, and identity systems, so one compromised account cannot disrupt the whole business. Human-centered training is equally important. Instead of generic security videos, employees should practice realistic help-desk scenarios, learn refusal scripts, and be rewarded for escalating suspicious requests. Companies should also reduce unnecessary public employee data and monitor identity-provider logs for unusual resets or MFA changes.

Barriers and Mitigation

Major barriers include cost, employee fatigue, pressure for fast service, and resistance to stricter verification. These can be reduced by designing procedures with employee input,

automating low-risk tasks, and tracking security quality alongside response speed. Leadership must make clear that slowing down a suspicious request is successful job performance, not failure.

Reflection and Conclusion

The MGM case shows why cybersecurity and social sciences must work together. Technical tools matter, but attackers target human expectations, workplace norms, and trust. A multidisciplinary approach helps organizations design systems that support better decisions instead of blaming individual workers after an incident. The key lesson is that people are not the weakest link; unsupported people are.

References

CISA. (2023, November 16). *Scattered Spider | CISA*. Www.cisa.gov. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a

Page, C. (2023, October 6). *MGM Resorts confirms hackers stole customers' personal data during cyberattack*. TechCrunch. https://techcrunch.com/2023/10/06/mgm-resorts-admits-hackers-stole-customers-personal-data-cyberattack/