Case Study: The 2023 MGM Resorts Cyberattack and the Psychology of Social Engineering

Joshua Martin

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Diwakar Yalpi

April 21, 2026

Introduction

September 2023 at MGM Resorts International a catastrophic attack occurred by a threat group that went by the name of Scattered Spider. However MGM Resorts as an organization was known for having very secure enterprise-grade defenses, regardless of this attackers were still able to breach through using a very low effort method: of which being voice phishing. Using OSINT (open-source intelligence), having access to platforms like LinkedIn, the attackers played the role as an employee and was able to manipulate the companies IT helpdesk into resetting an accounts multi factor authentication, allowing the attacker to gain access to credentials. (Muncaster, 2023) Not only does this incident signify the reality of attacks against our intelligence, but also shows that even with technological safeguards these efforts of protection can easily become ineffective when human behaviours are manipulated.

Analysis

Looking at this breach using psychology and sociology it shows why having social engineering skills is one of the top traits to have as a cyber threat actor. These attacks are able to skillfully exploit people's cognitive behaviour through different types of principles like authority, urgency, and compliance (Cialdini, 2021). Because of how they made themselves seem like a frustrated employee who needed immediate access, the attacker was able to hijack the cognitive decision of the helpdesk into giving the attacker what they wanted by making the situation seem rushed and urgent.

Sociologically the culture of the IT support structure itself is one of the most important roles in making sure vulnerabilities like this aren't breached. Helpdesks usually revolve around getting resolutions done as fast as possible while also making sure their customer service is 100%. However this in itself is a vulnerability, because the act of being helpful could play as a key

downfall for security protocols.

Proposed Solutions and Barriers

How can we mitigate the vulnerabilities? Firstly the organization should teach their employees about these social science insights directly to them, security practices and training are very important in a company especially MGM, so training the employees to challenge against suspicious behaviour should be a natural trait to have. A solution that could mitigate breaches like this are verification systems that require mandatory video call verification for multi step verification, which ends the urgency trait of the attacker all together.

Reflection

Looking at the MGM breach it shows how important it is to have an multidisciplinary approach in mind because of social engineering risks. Because even having the most robust security measure, it would be rendered useless if the behavioural and psychological weapons of attackers are ignored. So meshing together psychology into a company's current security protocols can upgrade the company's defense entirely, by making sure there is no “weak link”, erasing that blindspot entirely.

Conclusion

The attacks that took place at MGM Resort puts light on the fact that major cyber threats are not technical, but human problems. By webbing together strong security protocols with a better understanding of human behaviour, this will allow professionals in the field to have the skills to defend against being manipulated psychologically.

References

Cialdini, R. B. (2021). Influence, new and expanded: The psychology of persuasion. Harper Business.

Muncaster, P. (2023, September 15). MGM Resorts paralyzed by social engineering attack. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/mgm-resorts-paralyzed-social/