Cybersecurity Case Study: The MGM Resorts Social Engineering Breach

Student Name: Patrick Bays

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 04/21/2026

Introduction

In September 2023, MGM Resorts fell victim to a cyberattack orchestrated by the threat group "Scattered Spider". Unlike traditional breaches involving software exploitation, this incident began with a simple vishing (voice phishing) attack. Through pretexting, impersonating an employee identified by their LinkedIn profile, attackers convinced support staff to reset Multi-Factor Authentication (MFA) credentials. This allowed unauthorized access to administrative accounts, leading to a total system shutdown of hotel operations and gaming floors.

Social Science Perspective

From a psychological perspective, the breach exploited Authority Bias and Cognitive Load. Attackers created a sense of urgency, pressuring help desk agents to bypass existing protocols to assist a seemingly distressed higher-up. In high-pressure environments like this, the human brain often shifts from analytical skepticism to helpful compliance in order to resolve the conflict quickly. Sociologically, the attack exploited MGM's culture of hospitality. The guest-first mentality inherent to the resort industry likely inadvertently influenced internal IT. This created a cultural vulnerability where operational efficiency and helpfulness outweighed the need to abide by security protocols, allowing social engineers to manipulate staff who were trained to prioritize user satisfaction over strict verification.

Proposed Strategies

To address these vulnerabilities, MGM needs to take a multidisciplinary approach. On the technical side, they need to implement phishing-resistant multi-factor authentication (MFA) like using FIDO2-certified hardware tokens for all administrative accounts in order to ensure that even if a password is stolen via phishing/vishing, the account remains secure, because the secondary security challenge cannot be issued over the phone. For the social aspects, they could implement dual-authorization for high-risk identity changes. Requiring a second peer to verify MFA resets uses social pressure as a defense mechanism.

Identified Barriers

A primary barrier is user friction. Strict security protocols slow down support times, leading to employee frustration and potential deviant activity as they work around these protocols in the name of ‘efficiency’ to achieve work goals implemented by higher-ups that value numbers over quality. To overcome this, organizations need to foster a security culture where employees feel empowered to deny requests that don’t meet verification standards, rather than feeling pressured to accept every ticket that comes their way. They could do this by rewarding proactive reporting of suspicious calls rather than punishing failures.

Reflection

This case study demonstrates that cybersecurity is not necessarily just a problem of code and firewalls, that flawed human vulnerabilities can breach just as easily as code vulnerabilities. Integrating social sciences allows us to move beyond blaming users and instead working to design systems that account for cognitive biases. A multidisciplinary approach ensures that security measures remain steadfast against both digital exploits and the manipulation of humans.

Conclusion

The MGM breach serves as a reminder that the most sophisticated network defenses are only as strong as the human processes supporting them. By combining robust technical controls with the social aspects of employee psychology and sociology, organizations can build a more holistic defense-in-depth strategy to ward off attackers.

Works Cited

Elsawah, A. (2025, April 14). *Root cause of MGM hack, and how it could have been prevented*. The Security Cafe. https://www.lastweekasavciso.com/p/root-cause-of-mgm-hack-and-how-it

Eclypses. (2023, November 30). *The MGM resorts cyberattack: Hackers Steal Customer's personal data*. Eclypses Inc. https://eclypses.com/news/the-mgm-resorts-cyberattack-hackers-steal-customers-personal-data/