CASE STUDY: MGM RESORTS INTERNATIONAL CYBER BREACH Social Engineering Vulnerabilities & Organizational Risk Assessment

Chima C. Ozonwoye

Essex County College

ozonwoyechima@gmail.com

October 2024

Executive Summary

This report analyzes the September 2023 cyber-attack on MGM Resorts International, which exposed a critical vulnerability in modern enterprise security: the human element. Despite possessing sophisticated technical defenses, the organization suffered a catastrophic breach through a vishing attack targeting the IT help desk. Threat actors successfully leveraged basic employee information to bypass authentication protocols, gaining Super Administrator access to critical Okta and Azure environments. This incident demonstrates that even the most robust digital architecture remains fragile when social engineering vectors are left unaddressed.

The assessment highlights a recurring pattern of organizational failure, citing unheeded lessons from a 2019 breach and quantifying the recent operational impact at approximately $100 million in revenue loss. The report concludes that purely technical controls are insufficient against psychological manipulation. Strategic recommendations include the implementation of device trust verification systems and strict escalation procedures for credential resets to establish a resilient "human firewall" capable of withstanding future social engineering attempts.

1. Introduction

The September 2023 cyber-attack on MGM Resorts International revealed a fundamental truth about cybersecurity: social engineering is one of the most underestimated yet most concerning cyber-attack vectors in our digital age. Much like the Great Wall of China, which despite its impressive engineering was breached through human compromise, MGM's sophisticated digital systems proved susceptible to social engineering tactics. This case study demonstrates that a system built, run, maintained, and reliant on human interactions is inherently fragile, and no matter how robust the architecture, manipulation of its users can lead to security breaches. This cyber-attack on MGM Resorts International presents a critical case study of how social engineering vulnerabilities can bypass even sophisticated technical security measures. This analysis examines not only the technical aspects of the breach but raises essential questions about organizational competence, security culture, and the human elements that made this attack possible.

2. Critical Questions and Investigation Framework

Several critical questions must be addressed to understand the full scope and implications of this attack:

1. Was the incident a result of:
   - Management negligence?
   - Technical incompetence?
   - Organizational arrogance?
   - Systemic failures across multiple levels?
2. What improvements were implemented after the 2019 breach?

- Were employee training programs sufficient?

- How effective were technical security measures?

- Was there adequate focus on social engineering threats?

3. Post-2023 Attack Considerations:

- Have effective measures been implemented to prevent similar attacks?

- Are there safeguards against the potential misuse of stolen data?

- Has there been a fundamental shift in security culture?

3. Technical Analysis

3.1 Attack Vector and Progression

Initial Compromise:

- Vishing attack targeting IT help desk

- Basic employee information used for authentication

- Successful password reset obtained through social engineering

System Impact:

- Gained super administrator access to Okta

- Obtained Azure tenant Global Administrator privileges

- Widespread system shutdowns required to contain breach

3.2 Data Exposure

Compromised Information:

- Names and contact details

- Driver's license numbers

- Social Security numbers (limited cases)

- Passport numbers (limited cases)

- Potentially sensitive employee records

4. Critical Analysis: Beyond Technical Failures

4.1 Human Vulnerability Assessment

The attack demonstrates a critical oversight in security thinking. Just as a civilization's strength isn't solely measured by its walls but by its people's resilience, cybersecurity cannot be reduced to technical controls alone. The MGM case reveals how social engineering exploits the human element - the most adaptable yet vulnerable component of any security system.

4.2 Organizational Culture Analysis

When examining this breach, we must consider:

1. Training Effectiveness:
   - Were employees adequately prepared for social engineering attempts?
   - Did training programs address psychological vulnerabilities?
   - Was there regular testing of security awareness?
2. Response Capabilities:
   - Why did initial response measures fail to contain the breach?
   - How prepared was the organization for a social engineering attack?
   - Were lessons from the 2019 breach effectively implemented?

4.3 Future Security Considerations

Post-attack, organizations like MGM should consider partnering with security vendors who:

- Understand both technical and psychological aspects of security

- Consider demographic and cultural factors in training programs

- Provide comprehensive social engineering assessments

- Offer ongoing monitoring and adaptation of security measures

5. Recommendations

5.1 Immediate Actions

1. Implement enhanced authentication protocols
2. Deploy device trust verification systems
3. Establish strict escalation procedures for credential resets

5.2 Cultural and Training Improvements

1. Develop comprehensive social engineering awareness programs
2. Conduct regular security drills
3. Create clear incident response procedures
4. Foster a security-conscious culture

5.3 Long-term Strategic Changes

1. Regular security audits focusing on both technical and human elements
2. Continuous assessment of social engineering vulnerabilities
3. Development of robust incident response capabilities
4. Implementation of advanced authentication systems

Critical Side Notes: Unanswered Questions and Future Implications

The severity of the September 2023 attack and its similarities to the 2019 breach raises several critical questions that demand attention.

1. Effectiveness of Post-Attack Measures

While MGM claims to have implemented enhanced security measures and training programs, the effectiveness of these improvements remains questionable. The 2023 attack occurred despite alleged improvements following the 2019 breach, raising serious doubts about the organization's ability to learn from past incidents. The pattern suggests a concerning cycle where lessons from previous failures go unheeded.

2. Social Engineering Preparedness

The success of the vishing attack raises critical questions about MGM's social engineering preparedness:

- Are employees regularly tested with social engineering drills?
- Has the organization implemented robust verification protocols?
- Is there a culture of security awareness or merely superficial compliance?

Consider a scenario where remote workers, feeling isolated from their teams and under pressure to maintain productivity, become more susceptible to social engineering. An IT staff member, working remotely and dealing with multiple urgent requests, might be more likely to bypass security protocols when faced with a persuasive vishing attempt. This psychological vulnerability, combined with decreased vigilance in remote settings, creates perfect conditions for social engineering attacks to succeed.

3. Management Accountability

The breach potentially stems from a combination of:

- Management negligence in prioritizing security
- Technical incompetence in implementing robust solutions
- Organizational arrogance in assuming existing measures were sufficient
- Systemic failures across multiple organizational levels

The inability to anticipate and prevent this attack suggests a fundamental lack of awareness at the leadership level, where understanding and acknowledging security vulnerabilities should be paramount.

4. Cost Analysis

The financial implications are staggering:

- Estimated $100 million in revenue loss
- Immeasurable reputational damage
- Legal costs from multiple-class-action lawsuits
- Operational disruption costs

Yet, the investment required for proper security measures would likely have been a fraction of these losses. Like a small tear in a garment that becomes a major rip if not promptly repaired, preventive measures, though potentially costly, are far less expensive than breach recovery.

5. Future Vulnerability

Perhaps most concerning is the compound effect of the 2019 and 2023 breaches. The stolen data from both incidents could be used to orchestrate more sophisticated future attacks. Organizations must recognize that accumulating security measures isn't sufficient without proper implementation and cultural change - much like having sophisticated locks is useless if people prop the doors open.

Critical Recommendations Moving Forward

1. Enhanced Verification Protocols
   - Implementation of device trust systems
   - Strict multi-factor authentication
   - Callback verification for sensitive requests

2. Cultural Transformation

- Regular social engineering drills
- Comprehensive security awareness training
- Development of security-conscious culture

3. Management Reform

- Clear accountability structures
- Regular security audits
- Investment in preventive measures

4. Data Protection Strategy

- Protection against future attacks using stolen data
- Enhanced monitoring for suspicious activities
- Regular security posture assessments

The question remains: Will MGM and similar organizations learn to treat social engineering as a critical threat rather than an inconvenience? As the digital landscape evolves, the human element remains both our greatest vulnerability and our strongest potential defense.

6. Conclusion

The MGM attack serves as a stark reminder that at the peak of any empire, military strength protected resources and signaled civilization's power. Similarly, in our increasingly digital world, cybersecurity professionals play a crucial role in defending critical digital assets and infrastructure. However, this case demonstrates that even the strongest digital defenses can be compromised if the human element is not adequately protected.

The 2019 and 2023 MGM breaches highlight a concerning pattern where technical solutions alone prove insufficient. As we look to the future, organizations must consider not only their current security posture but also the potential long-term implications of compromised data from these breaches. The question remains: are there adequate measures in place to prevent stolen data from being used to orchestrate future attacks?

Moving forward, organizations must recognize that social engineering isn't just a technical cybersecurity issue, it's a human issue. The success or failure of security measures ultimately depends on building a culture of vigilance and education around cybersecurity. Without this foundation, even the most sophisticated technical defenses become as vulnerable as an empire with impressive walls but compromised guards.

The MGM attack highlights how social engineering threats require a holistic approach to security. Organizations must understand that technical solutions alone cannot prevent breaches when human vulnerabilities remain unaddressed. Success in cybersecurity requires a careful balance of technical controls, human awareness, and organizational culture.

Organizations must ask themselves not just if their technical security is adequate, but if their human firewall is equally robust. The true measure of security effectiveness lies not just in the sophistication of technical controls, but in the resilience of the entire system - including its human elements.

References

Ahern, B. (2023, October 5). MGM RESORTS UPDATE ON RECENT CYBERSECURITY ISSUE. Investors.mgmresorts.com. https://investors.mgmresorts.com/investors/news-releases/press-release-details/2023/MGM-RESORTS-UPDATE-ON-RECENT-CYBERSECURITY-ISSUE/default.aspx

1Password. (2024). What everyone got wrong about the MGM hack | 1Password. 1Password Blog. https://blog.1password.com/mgm-hack/

A Look Back at the MGM and Caesars Incident. (2024). Brown & Brown. https://www.bbrown.com/us/insight/a-look-back-at-the-mgm-and-caesars-incident/

APPENDIX A: 2026 Supplementary Visualization

Note: This visual guide was developed in 2026 to operationalize the "social engineering awareness" recommendations proposed in Section 5.2 of this report.

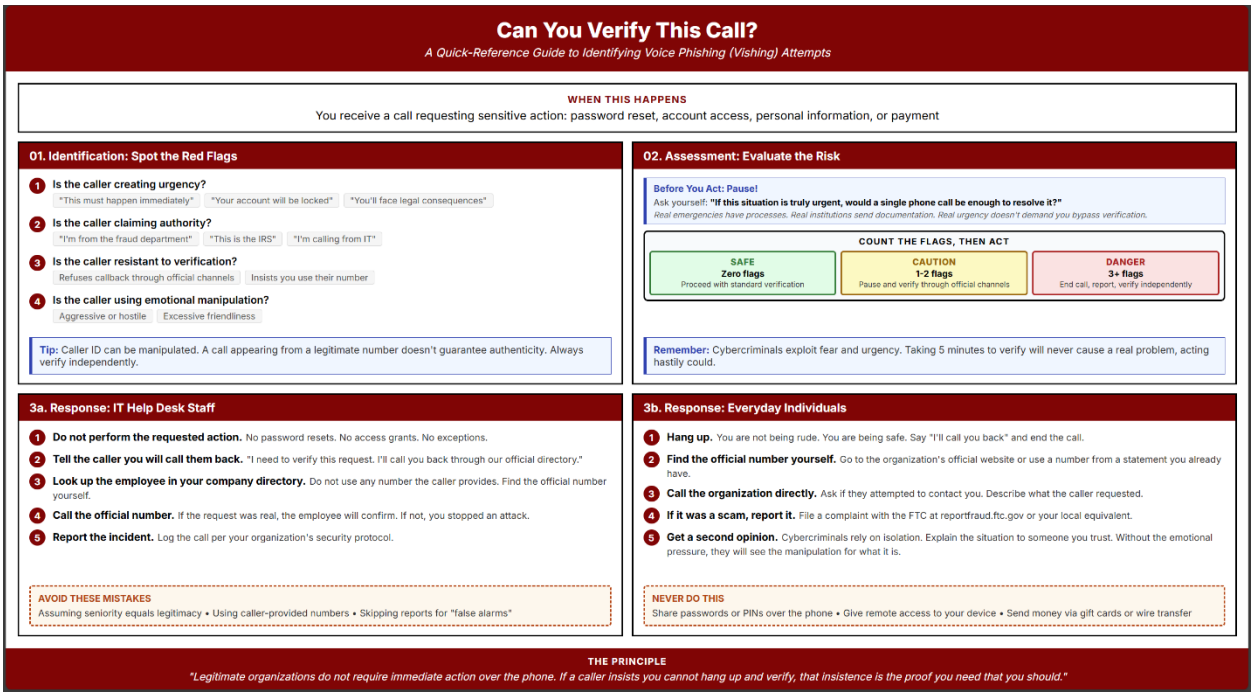

Figure A. 1 Vishing Verification Protocol (2026). A visual implementation of the "strict escalation procedures" recommended in Section 5.1.