

The MGM Ransomware Attack

Samuel Woodruff

Department of Cybersecurity, Old Dominion University

CYSE 462: Cybersecurity Fundamentals

Professor Bhanuka Mahanama

April 13, 2026

In September 2023, MGM Resorts experienced a large cyber attack that caused serious disruption for its locations across the United States. The cyber attack affected a number of different systems at the resorts such as hotel guest services, slot machines in the casinos, ATMs, and much more. The primary method of attack for this cyber attack sets it apart from typical cyber attacks in that it relied heavily on social engineering for it to be successful. Throughout this report, I will detail the MGM Resorts cyber attack, the vulnerabilities exploited, the primary methods of attack, the impact on the business and society, and different ways to help mitigate an attack like this in the future.

To understand the significance of the attack, it is important to first examine the background of MGM Resorts and their systems. MGM Resorts operates both hotel and casino locations around the world. According to MGM's website, their physical locations consist of "...31 unique hotel and gaming destinations globally" (MGM Resorts, n.d.). In addition to their physical locations, MGM Resorts operates one of the largest online sportsbooks today called BetMGM. MGM Resorts uses a multitude of different systems in order to provide their hotel, casino, and online sportsbook experiences to its customers. Some typical systems MGM Resorts uses include hotel reservation applications, payment systems, internal networks, mobile applications, and casino software. Like many large organizations, MGM Resorts makes use of several authorization and authentication systems to identify both guests and employees across its network. One system typically used to provide this security is Active Directory which manages a user's groups and permissions within a system. Many hackers seek to gain unauthorized access to systems by being granted greater privileges either by themselves or through the manipulation of others.

With the brief background of MGM Resorts and their systems in mind, the details of what happened in the cyber attack may now be examined. The attack happened over a period of multiple days, with anomalous activity appearing slowly in the beginning but worsening as time went on. According to Dirk Schrader of Netwrix, “It is believed that the attackers first breached the network on September 8” (Schrader, 2025). Disruptions in MGM Resorts’ services started out slowly, but rapidly worsened as hackers gained expanded access across different systems. As MGM Resorts began noticing the worsening anomalous activity, they were forced to take several of their services offline which disrupted normal business operations greatly. According to Fatima Gomez of Inszone, “Over several days, everything from slot machines to mobile check-ins was offline, forcing staff to process transactions manually” (Gomez, 2025). Being one of the largest entertainment businesses in the United States, having to process transactions manually with little technology is a massive disruption. In addition to disruption of MGM Resorts services, hackers were able to access thousands of customer’s personal information and encrypt it with ransomware. The customer information accessed by hackers included sensitive information such as credit card numbers, full names, birthdays, and much more. The attack lasted for several days and greatly disrupted MGM Resorts operations across the United States causing significant financial losses, left customers with their sensitive information compromised, and a degradation in brand trust.

One of the most important parts to examine about the MGM Resorts cyber attack is how hackers were able to gain access and carry out their attack successfully. According to Fatima Gomez, “Cybersecurity researchers linked the MGM hack to Scattered Spider, a subgroup of the ALPHV (BlackCat) ransomware gang” (Gomez, 2025). The key method of exploitation in this attack was Scattered Spider’s use of social engineering in order to gain unauthorized access to

MGM Resorts' systems. The hackers from Scattered Spider began their attack by utilizing a social engineering attack called vishing. Vishing, as defined by Cisco, is "... short for voice phishing, uses fraudulent phone calls to trick victims into providing sensitive information, like login credentials, credit card numbers, or bank details" (Cisco, n.d.). To successfully carry out the vishing attack, Scattered Spider followed a few different steps. First, Scattered Spider hacks researched information on actual MGM employees through websites like LinkedIn and eventually chose an employee to impersonate. (Schrader, 2025). The hackers, impersonating an actual MGM employee, contacted the company's IT help desk and successfully tricked them into providing login credentials. (Schrader, 2025). Schrader explains, "Using the obtained credentials, Scattered Spider gained administrator privileges to MGM's Okta and Azure tenant environments" (Schrader, 2025). From there, Scattered Spider hackers were able to move laterally across MGM Resorts' systems and gain access to sensitive information, severely hampering the operations of the business. Being a ransomware-focused group, Scattered Spider was then able to deploy BlackCat/ALPHV ransomware, encrypting "...approximately 100 ESXi hypervisors within MGM's network" and additionally claimed "...to have exfiltrated 6 TB of customer information..." (Schrader, 2025). Scattered Spider then threatened to keep the encryption of critical services in place as well as publicly leak sensitive customer information in order to extract a ransom payment from MGM Resorts which ultimately was unsuccessful.

Following the cyber attack, MGM Resorts faced several different kinds of consequences in the aftermath. Due to disruptions from the cyber attack, MGM Resorts reportedly suffered roughly \$100 million in financial losses in the third-quarter of 2023. (Gomez, 2025). Like other cyber attacks, MGM Resorts also suffered significant loss in consumer trust following the cyber attack. According to Steve Weisman of Forbes, customers affected by the cyber attack were

awarded \$45 million in a class action lawsuit against MGM Resorts for negligence resulting in the cyber attack. (Weisman, 2025). Lastly, Gomez reports “MGM committed \$50 million to upgrade endpoint protection, cloud security, and employee training to combat future MGM resorts cyber attacks” (Gomez, 2025). In all, the cyber attack resulted in significant financial damages for MGM Resorts and an overall degradation in consumer trust.

Being one of the more notable cyber attacks in recent memory, the MGM Resorts cyber attack had a great impact on society as a whole. The attack helped prove that significant technological integration and reliance can prove to be greatly disruptive if and when attacked. Many organizations either lack the proper infrastructure, planning, or ability to carry on regular operations due to their dependence on technology. For that reason, it’s extremely important to have the most robust security possible and this attack helped underscore that importance. Another massive impact on society resulting from this attack is that it helped show that the human aspect of cybersecurity remains one of the largest vulnerabilities an organization can have. The Scattered Spider group did not have to use a technological exploit in order to gain access to MGM Resorts’ systems, but instead relied on simple trickery through vishing. All the hackers had to do was look up an employee on LinkedIn and then successfully pose as that employee to the IT helpdesk in order to gain near unimpeded access to a massive organization. The simpleness of Scattered Spider’s social engineering success proves that organizations and society as a whole must invest more into cybersecurity education and training. An organization’s cybersecurity practices and services can be as robust as possible, but still be thwarted by hackers taking advantage of the human aspect. For those reasons, the MGM Resorts cyber attack proved to be significantly impactful to society.

To prevent similar attacks like the MGM Resorts cyber attack, organizations can implement several different forms of mitigation. Firstly, organizations can require more robust multi-factor authentication. Multi-factor authentication requires users to provide an additional form of authentication in addition to having the correct login credentials, typically in the form of an authenticator application or providing a code. If implemented correctly, multi-factor authentication has the potential to thwart cyber attacks early on or at the very least slow them down enough to be detected. Similarly, another step organizations can take is to have greater verification protocols for the IT helpdesk. This can be done by requiring multiple forms of identification in order for the IT helpdesk to know for certain who they are speaking to. Another way to mitigate an attack like this is to ensure everyone in the organization has least privilege access. This ensures that individuals throughout the organization only have access to the permissions they absolutely need for their job function and zero access to those they do not. Lastly, organizations should fund greater cybersecurity awareness training in order to help mitigate the vulnerabilities caused by the human aspect.

The 2023 cyber attack on MGM Resorts helps show that modern attacks utilize a blend of different exploits targeting technology and human behavior. Through use of social engineering, hackers were able to gain access to a massive business and not only interrupt its daily operations, but also gain access to sensitive information from thousands of customers. This attack helps show that organizations can spend millions on cybersecurity technology in order to thwart attacks but still remain vulnerable from human behavior. As cyber attacks grow more sophisticated and AI-integrated, organizations must address cybersecurity with a more rounded approach that focuses on strong policies, technological innovation, and employee education.

Works Cited

Cisco Systems. "What Is Vishing?" *Cisco*,
<https://www.cisco.com/site/us/en/learn/topics/security/what-is-vishing.html>. Accessed 13 Apr. 2026.

Forbes. "MGM Ransomware Attack Update." *Forbes*, 12 Mar. 2025,
<https://www.forbes.com/sites/steveweisman/2025/03/12/mgm-ransomware--attack-update/>.
Accessed 13 Apr. 2026.

Inszone Insurance Services. "Cyberattack MGM Resort Explained." *Inszone Insurance*,
<https://inszoneinsurance.com/blog/cyberattack-mgm-resort-explained>. Accessed 13 Apr. 2026.

MGM Resorts International. "Company Overview." *MGM Resorts*,
<https://www.mgmresorts.com/en/company.html>. Accessed 13 Apr. 2026.

Netwrix. "MGM Cyber Attack." *Netwrix*,
<https://netwrix.com/en/resources/blog/mgm-cyber-attack/>. Accessed 13 Apr. 2026.

