CYBER ATTACKS

A $15 million Las Vegas casino heist without using a gun

By Richard Wickliffe, CPCU, ARM November 16, 2023, 3:49 p.m. EST5 Min Read

- Facebook
- Twitter
- LinkedIn
- Email

On the Las Vegas Strip, MGM Resorts' 12 casinos went dark on September 10, 2023. The occurrence comprised disabled computers, dead gaming machines, malfunctioning room keys, stuck elevators and strange charges on guests' accounts.

Four days earlier, Caesars Entertainment, their primary competitor with nine Vegas casinos, had surrendered $15 million to the same criminals.

Were these heists performed by George Clooney's *Ocean's Eleven* crew, with a meticulously planned scheme? No, the assaults were reportedly carried out by

cybercriminals aged 19 to 22, scattered across the United States and United Kingdom, likely while seated in the comfort of their homes.

The day after the MGM attack, they had to disclose that a "cybersecurity issue" had severely impacted the organization. To halt further damage, the company temporarily shut down its systems. However, the attackers began lurking within MGM's networks for several days before they made their ransom demands.

MGM Resorts' CEO Bill Hornbuckle made the bold decision not to pay the ransom. This option came with substantial risks, as experts estimated that MGM would lose up to $8.4 million *per day* until its systems could be fully restored. According to *Fox Business*, the losses could amount to 10% to 20% of the company's combined revenue.

In stark contrast, when Caesars Entertainment fell victim to an attack just days earlier, they made the controversial choice to pay $15 million in ransom (negotiated from the original $30 million demand).

So how did the news leak? One might think companies would rather keep intrusion reports confidential to avoid negative publicity. The attacks were disclosed because the companies were required to file a Form 8-K with the U.S. Securities and Exchange Commission. The SEC mandates the filing of an 8-K to disclose significant events that affect shareholders, typically within four business days. Caesar's 8-K filing about the cyberattack and ransom payment stated they "do not expect that it will have a material effect on the Company's financial condition…"

However, MGM's 8-K report projected a negative impact from the cyberattack estimated at $100 million, in addition to $10 million in expenses, which included costs for IT consulting and legal fees.

To pay or not to pay

A challenging dilemma: Should you pay the ransom or not? MGM had to consider an

$8.4 million daily loss while their systems were down versus a one-time $15 million ransom to make the problems vanish. But could halting the financial hemorrhage be viewed as a weakness, potentially luring cybercriminals back? Is there any honor among these digital outlaws?

MGM's claims the choice not to pay the ransom was influenced by the Federal Bureau of Investigation. Similar to the "we don't negotiate with terrorists" mindset, the FBI discourages paying ransoms to cybercriminals, as it can encourage more attacks.

How did the attack happen?
It's widely speculated the cybercrime group known as "Scattered Spider" attacked both companies. The young hackers, based in the U.S. and U.K., reportedly used ransomware created by "BlackCat" aka "ALPHV," one of the most complex malware programs.

Ironically, their initial intrusion was more low-tech. The group specializes in social engineering, where they manipulate employees into performing actions by mimicking people or companies the victim has a relationship with. Also known as "vishing" (voice phishing) the hackers gain access to systems through convincing phone calls rather than fraudulent emails.

Humans are usually the weakest link in cybersecurity. Here, it seems that open sources and a persuasive phone call were sufficient to penetrate MGM's networks. According to a recent Vox article, hackers likely obtained an employee's information from LinkedIn, then used it to impersonate the employee in a call to MGM's IT help desk to gain further access. Imagine a scenario as simple as requesting a password reset.

Scattered Spider proceeded to steal and encrypt MGM's data, demanding a ransom in cryptocurrency to release it.

MGM incurred substantial damages, including the estimated $110 million in losses and expenses. In addition, the occupancy rates at MGM hotels took a significant hit, with an 88% drop from the prior month, according to *The New York Post*. Ongoing losses are probable because the hackers also accessed names, addresses, birthdates, and driver's license numbers of certain customers. In response, MGM CEO Hornbuckle assured customers that the hackers had not accessed credit or bank account numbers due to their swift response.

Both casinos are facing a combined six class-action lawsuits thus far as a result of the cyberattacks, alleging the companies were negligent in protecting its customers' personal information during the attacks. Caesars' senior vice president of infrastructure and cybersecurity, John Roskoph, exited shortly after the attacks.

Were the losses insured?
MGM claims they had cybersecurity insurance sufficient to cover the losses. The company was reportedly covered by a $200 million cyber insurance policy, covering ransom payments and business interruption. They claim the overall impact of the attack wouldn't hurt their annual performance, according to *The Wall Street Journal*.

Sources claim that AIG wrote the primary layer on MGM Resorts' $200 million policy, with Beazley serving as the first excess carrier, and placements syndicated across multiple insurers. By chance, the same carriers reportedly insure Caesars Entertainment as well.

More significantly, cyber insurance exists to help companies like MGM and Caesars regain customer confidence. As proof, the day after MGM announced it had enough cybersecurity insurance to cover the losses, shares of MGM Resorts rose 5.4%, up from a 16% drop in the prior month, according to *MarketWatch*.

These attacks demonstrate that companies, even those presumed to have bulletproof security –e.g., the world's largest casinos – remain vulnerable. Moreover, the publicized breaches might result in an increase in vishing attacks as other criminal groups watch from the sidelines.

Considerations
· Cyber Insurance: Many policies cover ransom payments, data recovery, business interruption, notification costs, legal fees, and settlements.

· Address the core vulnerability: Verify identities, use unique passwords for multiple systems, and implement multi-factor authentication.

· Vishing tests: Should we increase human caller-based "vishing" tests to identify training gaps? It seems the common training relies heavily on phishing tests.

The Las Vegas cyberattacks should serve as a wake-up call for boards, underscoring the fact that anyone can fall victim to cyberattacks if proper controls aren't in place. Cyber incidents should be regarded as inevitable, and executives must ensure they are prepared to effectively manage the risks when such an attack occurs.

Richard Wickliffe, CPCU, ARM
Insurance Executive

CYBER ATTACKS **CYBER SECURITY** **RANSOMWARE**