Don't Gamble With Your Cybersecurity and Incident Response Plan: Lessons Learned from the Las Vegas Ransomware Attacks

Article
Amundsen Davis Cybersecurity & Data Privacy Alert
September 21, 2023

Typically, we beat the drum of the need to prepare for a data incident—anything from a full-blown ransomware attack to an employee accidently sharing data with the wrong person—by having your Incident Response Plan developed and at your fingertips. Companies may view this advice through the lens of concern over loss of personal data to threat actors.

Even today, a likely misconception is that the monetary loss from ransomware attacks or other cyber incidents is the taking of personally-identifiable information—that the reason bad actors can ask for a 6- or 7-figure ransom is because employee or consumer personal information has been taken and businesses (and people) will pay a hefty sum for the deletion or return of that data. Not so.

In today's threat landscape, the more impactful part of a cyberattack—and the screw that threat actors can turn to ask for millions in ransom—is the business interruption damage and the related business reputation costs. (For more on the business interruption and the responsibility of directors and officers, check out our corporate blog.)

Case and point? On September 10, 2023, certain major hotels in Las Vegas, including the Bellagio and MGM Grand, were left with faulty door locks, inoperable slot machines and other problems in the wake of a cyberattack. Resolution of these issues is ongoing—and, at the same time, Caesars Entertainment acknowledged it was also the target of a cyberattack.

From a cybersecurity standpoint, these incidents are notable for at least two reasons that go beyond the typical considerations. First, the reporting about the attack does not highlight exfiltration or taking of personal information but rather the interruption to the businesses. Hackers rendered doors to the Bellagio's and MGM Grand's casinos and hotels unusable. Slot machines and ATM machines were also inoperable; elevators couldn't be used; and, customers had to wait

PROFESSIONALS

Molly A. Arranz
Partner

RELATED SERVICES

Cybersecurity & Data Privacy

AMUNDSEN DAVIS

hours to check into rooms. Even the company's website went down.

Second, though it's not clear how the threat actors were able to access and compromise MGM Resorts' system, one theory is that the ransomware group "ALPHV," also known as Black Cat, found its foothold via LinkedIn. They located an employee profile on that social media forum then called the Help Desk and leveraged information via a short conversation with the Help Desk.

These recent Vegas cyberattacks raise an additional motivator to develop an Incident Response Plan, today.

What does that mean for you? Some takeaways:

1. Lose the philosophy or way of thinking that you "don't have much personal information," so you won't be a target of a cyberattack. Rather, your need to keep your business up-and-running could be a significant motivator to pay a sum to resume business as usual. No business is safe.
2. The recent Vegas cyberattacks raise an additional motivator to make a plan, today.
3. Prepare, prepare, prepare. In the wake of a cyberattack that has shut your system down is ***not*** the time to try to figure out your emergency response plan. Get your incident response plan ready now.
4. Business interruption of your day-to-day activities (think about simply an inability to get invoices out and deposit payments coming in) equates to big monetary losses– not just for your company, but for your business and industry partners. This should be a motivator to ensure you are evaluating what layers of security you have in place to limit this exposure. Training of your employees to avoid the sophisticated means of potential infiltration is also critical.