NEAL GERBER EISENBERG

CLIENT ALERT

Cybersecurity Risks and Regulatory Challenges Impact Hospitality Industry

By: Kate Campbell, Alfred Tam, David Wheeler and Josh Hanson

November 21 , 2024

The hospitality industry is a prime target for cyber criminals, due in part to the high volume of sensitive guest data, including financial information, that companies maintain. Almost one-third of hospitality organizations have reported a data breach in their company's history, costing an average of approximately $3.4 million, according to a 2023 report by cybersecurity provider Trustwave.

Recently, high-profile data breaches experienced by MGM Resorts and Caesars Entertainment have dominated headlines. MGM Resorts reportedly suffered over $100 million in costs as a result of a cyberattack in 2023, causing a very public impact on its guest operations. The MGM hack was the result of a social engineering attack by a well-known cybercriminal gang. The attacker called the company's helpdesk and impersonated an employee. The attacker convinced the helpdesk to give the attacker access to the impersonated employee's account, which had high-level access privileges on MGM's systems. Then, in 2023, Caesars suffered a ransomware attack and paid a $15 million ransom to prevent the attacker from publishing the stolen data. The threat actor initially compromised a third-party IT vendor using social engineering techniques and then used the vendor's access rights to obtain Caesars' loyalty program database.

These breaches highlight the importance of implementing and maintaining comprehensive cybersecurity programs to avoid operational and reputational damage. However, those are not the only risks hospitality organizations face. Recent action from the Federal Trade Commission (FTC) highlights the regulatory risks the hospitality industry also faces as a result of a data breach.

The FTC recently announced a multi-million dollar settlement with another major hotel chain for allegedly inadequate data security practices that led to data breaches impacting hundreds of millions of customers. This announcement underscores just how critical it is for businesses to ensure they have appropriate cybersecurity practices in place and deliver on their cybersecurity promises.

Between 2014 and 2020, the hotel chain suffered three data breaches and the FTC subsequently brought a complaint against the chain for violation of the Federal Trade Commission Act's prohibition on "unfair or deceptive acts or practices." Among the chain's many alleged "unfair" cybersecurity failures were:

1. Failure to ensure that employees use adequately strong passwords;
2. Failure to patch outdated systems and software;
3. Failure to monitor network activity to detect unauthorized activity;
4. Failure to maintain adequate access controls to ensure that employee access was granted and terminated appropriately;
5. Failure to maintain adequate firewall controls to prevent unauthorized connections from outside its networks;

6. Failure to segment networks to prevent intruders from moving between systems; and

7. Failure to use multifactor authentication.

In addition to the alleged cybersecurity failures noted above, the FTC alleged that the hotel chain engaged in deceptive practices by assuring their customers, via the privacy policies posted on their websites, that they used "appropriate safeguards" to protect customers' personal information.

The settlement included not only a multi-million dollar penalty payment but also a series of mitigation measures, such as a requirement to implement data minimization and deletion policies to ensure that data is not retained longer than necessary, a new comprehensive information security program with annual compliance certification for the next 20 years, and mechanisms for customers to request a review of their account activity and deletion of their personal information. It is important to note that the FTC's power to enforce cybersecurity standards extends beyond the hospitality industry, to any business that engages in what the FTC considers unfair and deceptive practices in or affecting commerce. Essentially, if a business's unreasonable cybersecurity practices cause or are likely to cause a consumer injury, the FTC may have regulatory authority.

While cybersecurity may, at times, feel like a moving target, this settlement illustrates what the FTC considers reasonable and appropriate security measures. If a business does not have in place the measures the FTC called out above as missing, it should consider strengthening its cybersecurity program. In addition, the FTC has issued guidance related to cybersecurity controls and the use by businesses of the National Institute of Standards and Technology (NIST) Cybersecurity Framework that are instructive on the cybersecurity standard of care. Lessons learned from MGM and Caesars also emphasize the importance of training employees on cybersecurity practices and vendor management programs that evaluate and mitigate cybersecurity risks faced by vendors. This is especially true as we continue seeing cyberattacks that are initiated within a vendor's systems before moving laterally into its customers' systems. In addition, the FTC's actions make clear that it is not enough to pay lip service to data security in privacy policies. Businesses must ensure that they are ready and able to follow through on those promises made to consumers.

This alert was authored by

Kate Campbell | (312) 269-2964 | kcampbell@nge.com

Alfred Tam | (312) 269-8461 | atam@nge.com

David Wheeler | (312) 269-5328 | dwheeler@nge.com

Josh Hanson | (312) 269-5982 | jhanson@nge.com

If you need assistance developing or improving your cybersecurity practices, please contact your Neal, Gerber & Eisenberg attorney, or a member of our Cybersecurity & Data Privacy team—Kate Campbell, Alfred Tam, David Wheeler and Josh Hanson.

This client alert is the first in a series from the NGE Hospitality Industry Team addressing developments and recent news in the hospitality industry.

The NGE Hospitality Industry Team is an inter-disciplinary group focused on serving the diverse legals needs of hospitality owners, operators, and investors to achieve their business goals. The group collaborates to ensure our clients are well-informed on industry trends and ready to address both opportunities and challenges.

CLIENT ALERT