Cyberattack on Luxury Resort Should Put Hospitality Industry on High Alert

Insights
7.06.22

Cybercriminals are finding new ways to hold their victims hostage – and a recent cyberattack on a luxury resort should serve as a warning for your business. A June 15 media report revealed that one of Oregon's premier resorts, The Allison Inn & Spa, recently fell prey to a ransomware attack that left its employees' and guests' personal information exposed for the world to see. What's unique about this particular cyberattack is that the stolen information – which includes data from 1,500 employees and more than 2,500 guests, including dates the guests stayed at the hotel as well as employees' birthdays, phone numbers, and Social Security numbers – was posted on the public internet in easily searchable form. Typically, stolen confidential information such as this is only published on the "dark web" and is not as easily retrieved through any type of online searches. What does your business need to know about this new tactic – and what should you do to prevent such an attack?

New Tactic Reveals New Dangers

While the methods the cybercriminals used against The Allison may have been novel, their aim was typical: they were hoping to force the business to pay them a ransom. A cyberthreat analyst interviewed for the media report surmised that the public release of the confidential guest and employee data may have been an "experiment" to see whether it could further ratchet up pressure on the business to pay out the ransom. "They're likely doing this to see how much it moves the needle in their favor," said Brett Callow from Emsisoft. "Their intention may not simply be to try to squeeze the money out of The Allison. It may also be to pressure their future victims who look at what happened to the Allison and think, I don't want to go through that."

That means this new tactic may be a trend we see from cybercriminals looking to extort their victims in future ransomware attacks. The only (arguably) potential upside of this new public method of cyberattack is that individuals may be able to find out first-hand if their private information has been compromised, rather than wait to hear about it at a later date from a third-party, or pay a vendor to search the dark web for evidence that data has been leaked or made available for sale.

What Should Your Business Do?

In light of this incident, resorts across the country should be prepared to implement comprehensive cybersecurity risk management processes. If your business becomes the victim of a cybersecurity

attack, your cyber-incident response plan should be immediately deployed to take the following steps:

- Determine what systems were impacted and immediately isolate them;
- If affected devices cannot be removed from the network (or if the network cannot be temporarily shut down), secure the network by powering down infected devices to avoid any further spread of the ransomware infection;
- Triage impacted systems for restoration and recovery;
- Engage your internal and external stakeholders;
- Retain legal counsel to provide guidance in responding to the incident, including recommendations regarding potential data breach notification obligations and reporting requirements;
- Retain a third-party incident response provider with experience in data breaches; and
- Report the incident to law enforcement.

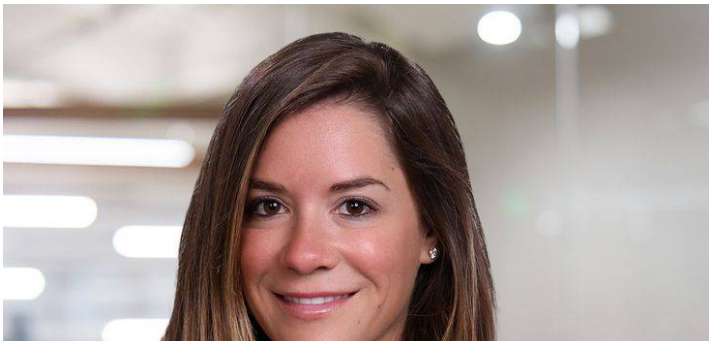
In addition, companies should consider deploying multifactor authentication in order to gain access to company networks, provide robust cybersecurity training to all employees on an annual basis, and maintain offline, encrypted backups of all internal data.

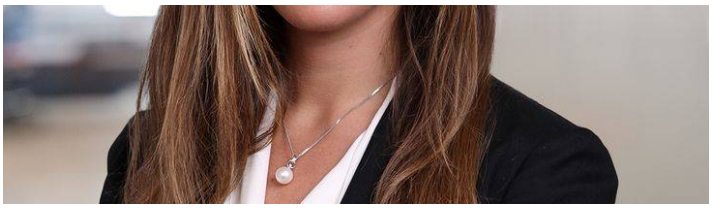
If you have cyber-insurance, you should also notify your carrier in a timely fashion to maximize the likelihood of coverage for costs associated with remediating and responding to the breach.

Conclusion

Fisher Phillips will continue to monitor any further developments in this area as they occur, so you should ensure you are subscribed to Fisher Phillips' Insight system to gather the most up-to-date information. If you have any questions regarding how cybersecurity threats could impact your organization, or best practices for mitigating the risk of those threats, please consult your Fisher Phillips attorney, the author of this Insight, or a member of Fisher Phillips' Privacy and Cyber Practice Group or our Hospitality Industry Practice Group.

Related People





Monica Snyder Perl
Partner
617.532.9327
Email

Service Focus

Privacy and Cyber

Industry Focus

Hospitality