Gregory & Appel Insurance Announces Cybersecurity Risk Management Strategies

The New Age of Hospitality Risk: Navigating Cybersecurity and Social Engineering Threats

Matt Stauffer, Senior risk advisor, Gregory & Appel Insurance

INDIANAPOLIS, IN, UNITED STATES, December 10, 2024 / EINPresswire.com/ -- By Matt Stauffer, Senior Risk Advisor

In today's digital world, cyber risks are on the rise, especially in the form of social engineering attacks. Hospitality businesses like resorts, timeshares, and property management companies are prime targets for these schemes, making it essential to stay proactive. Social engineering—where cybercriminals manipulate individuals to reveal sensitive information or take actions that compromise security—has become a leading threat. Common tactics include phishing emails, impersonation, and fake payment requests designed to gain unauthorized access to valuable information.

To address these risks, insurers are increasingly adding sublimits specifically for social engineering within cyber policies. Sublimits place a cap on payouts for specific types of claims, separate from the main coverage. For instance, a policy might have a $1 million overall limit, but a sublimit of $100,000 for social engineering attacks, meaning any claim related to social engineering would max out at $100,000. It's important to understand these sublimits as they reveal what's actually covered for specific threats and help identify any gaps that might need additional coverage or higher sublimits.

Types of Cyber Breaches and Realistic Claim Scenarios for Hospitality Businesses

Gregory & Appel Insurance

1. Phishing Scams Targeting Employees

•Situation: An employee at a property management company receives an urgent email from what appears to be a trusted vendor, requesting immediate payment for services. Without thinking, the employee clicks a link in the email, unknowingly sharing login details that allow the attacker access to sensitive financial data. The hacker uses these credentials to make unauthorized transactions totaling $150,000.

•Claim and Sublimit Impact: If the company's cyber policy has a $1 million limit but only $100,000 for social engineering claims, the business would be reimbursed up to $100,000, leaving it responsible for the balance. This scenario highlights the importance of reviewing sublimits in cyber insurance.

> To address these risks, insurers are increasingly adding sublimits specifically for social engineering within cyber policies."
>
> *Matt Stauffer, Senior Risk Advisor*

•Actionable Tip: Regular phishing awareness training for employees can go a long way in preventing these incidents. Make it a habit to simulate phishing tests as part of training and encourage employees to report suspicious messages to IT.

2. Ransomware Strikes During Busy Season

•Situation: During peak season, a resort's systems are attacked by ransomware, encrypting guest data and locking the team out of essential booking systems. Hackers demand a ransom of $300,000 to restore access, disrupting operations and causing revenue loss.

•Claim and Sublimit Impact: Ransomware sublimits often cap payouts for these incidents. For instance, if the policy caps ransomware claims at $200,000, any costs above this fall to the business. This makes it crucial to understand ransomware-specific coverage.

•Actionable Tip: Schedule regular system backups and store them offline. This simple step can be a lifesaver in getting systems back up and running without paying ransoms. Also, keep software up-to-date to guard against vulnerabilities that hackers exploit.

3. Data Breaches from Third-Party Vendors

•Situation: A resort's third-party booking software provider is breached, exposing guest data like credit card details and booking information. The breach incurs expenses for notifying guests, legal fees, and other costs.

•Claim and Sublimit Impact: Many policies have sublimits for third-party data breaches. For example, a $500,000 sublimit on third-party claims caps what the insurer will cover, even if the policy's overall limit is higher.

•Actionable Tip: Include third-party vendors in your regular security reviews. Ensure vendors

adhere to robust security practices and hold adequate insurance, so everyone's prepared in case of a breach.

Practical Cybersecurity Tips for Resorts, Timeshares, and Property Management Companies

Investing in these cybersecurity practices can go a long way in protecting your business and mitigating financial risks. Here's a guide to practical measures that are particularly relevant for hospitality businesses:

- Choose a Cyber Insurance Policy that Covers Your Needs: Hospitality businesses need comprehensive cyber insurance that covers a range of incidents, such as ransomware, data breaches, and social engineering. Look closely at sublimits for each type of claim. If handling large financial transactions is a regular part of business, consider a higher social engineering sublimit to align with your risk profile.
- Keep Cybersecurity Training on the Agenda: Employees are often the first line of defense. Regular training on identifying phishing emails, safeguarding passwords, and verifying unusual requests can significantly reduce vulnerability to social engineering. Make training interactive and keep it updated to reflect the latest cyber threats.
- Add Multi-Factor Authentication (MFA): MFA is an effective way to secure accounts. It requires two forms of identification to log in, meaning even if login details are compromised, access remains restricted. MFA is especially useful on systems that handle sensitive information or financial transactions.
- Schedule Regular Security Audits: Audits uncover vulnerabilities that could otherwise go unnoticed. Consider extending audits to include third-party vendors, whose security practices can impact your own. A proactive approach with audits helps to catch and fix issues before they escalate.
- Have a Crisis Response Plan Ready: When a breach occurs, a well-thought-out crisis response plan can make all the difference. Outline steps for notifying affected individuals, coordinating with IT and legal teams, and keeping the public informed if necessary. This preparedness can help minimize financial impact and reassure clients that the situation is under control.
- Review Vendor Contracts for Cybersecurity Standards: Third-party vendor breaches are increasingly common, so it's essential to review vendor contracts for solid cybersecurity practices. If possible, work only with vendors who carry their own cyber insurance—this additional protection can shield your business from unforeseen breaches and reduce liability.

Building a Cyber-Resilient Future

Cyber threats are constantly evolving, posing ongoing challenges for hospitality businesses. Taking a proactive approach with the right technology, regular employee training, and cyber insurance tailored to your needs allows resorts, timeshares, and property management companies to build a solid defense.

Investing in these measures now is a commitment to protecting not only your business but also the trust and security of the guests and clients you serve. With the right mix of technology, training, and policy coverage, hospitality businesses can confidently face the ever-changing cyber

landscape.

About Gregory and Appel
Gregory & Appel is an independent risk management advisor helping people and businesses navigate the complexities of insurance and employee benefits. As your partner, we'll help alleviate risk and strengthen resilience while uncovering pathways for continued growth and success.

For more information, please contact:
MStauffer@gregoryappel.com or visit https://www.gregoryappel.com/resorts for more information.

Matt Stauffer, Senior Risk Advisor
Gregory & Appel Insurance
+1 765-617-1077
email us here
