ASIAN SCHOOL OF CYBER LAWS

Cyber Security Checklist for Hotels and Casinos: 20 Questions to Ask

Tick each question you can answer with a confident yes. Every unticked box is a place to start.

VISIBILITY

01 ☐ Do we have an inventory of every connected system at each property, including locks and casino systems?

02 ☐ Do we know which vendors and franchisees connect to our systems?

03 ☐ Do we know where all our guest data is stored?

ACCESS

04 ☐ Do help desks, including outsourced ones, verify identity strongly before resets?

05 ☐ Is phishing-resistant MFA used for administrators and remote access?

06 ☐ Is MFA enabled on our booking platform and travel partner accounts?

NETWORK

07 ☐ Are guest Wi-Fi and in-room devices separated from operational systems?

08 ☐ Are payment systems separated from other property and corporate systems?

09 ☐ Are our door lock systems updated and using secure keycard technology?

DETECTION

10 ☐ Do we monitor identity systems around the clock for suspicious changes?

11 ☐ Would we detect large amounts of guest data leaving the network?

12 ☐ Would we spot malware on point-of-sale systems?

RESILIENCE

13 ☐ Are backups of identity, virtualisation and core systems stored offline and tested?

14 ☐ Could our properties check guests in, issue keys and take payments manually?

15 ☐ Do we have a plan for running casino operations during a system outage?

RESPONSE

16 ☐ Have we decided in advance how we would handle a ransom demand?

17 ☐ Do we have a plan for communicating with guests during an outage or breach?

18 ☐ Have we run a ransomware exercise across properties in the last 12 months?

PEOPLE AND GOVERNANCE

19 ☐ Are help desk, front-desk and casino staff trained to spot social engineering?

20 ☐ Does the board treat cyber risk as a risk to guests and operations?