Cyber Risk Exposure Scorecard – Hospitality

The following cybersecurity scorecard is tailored to the hospitality industry. Its purpose is to evaluate the level of cybersecurity readiness and resilience in organizations operating in this sector. With technology playing such a crucial role in providing seamless services and ensuring guest and client satisfaction, it is of utmost importance for hospitality businesses to prioritize the protection of sensitive information and systems. This scorecard covers critical areas such as governance and policies, network and infrastructure security, data protection, vendor management, and security monitoring and testing. By assessing these aspects, organizations can determine their cybersecurity posture, identify potential vulnerabilities and implement necessary safeguards to mitigate risks.

Please assign a score from 0–5 for each question based on your organization's compliance or implementation level. A higher score indicates a better cybersecurity posture. Consistently evaluating and updating the scorecard will aid in monitoring progress and pinpointing areas for enhancement.

WHEELER & TAYLOR
SINCE 1871

Questions	Score
Network Security	
Is there an up-to-date firewall in place to protect the network from unauthorized access?	
Is wireless network security properly configured with strong encryption and authentication mechanisms?	
Are intrusion detection and prevention systems (IDPS) deployed to identify and respond to potential threats?	
Data Protection	
Is sensitive customer data, such as credit card information, encrypted during transmission and storage?	
Are regular data backups performed, and is the restoration process tested?	
Are there secure storage and access controls for sensitive customer information?	
Payment Card Industry Data Security Standard (PCI DSS) Compliance	
Is the organization compliant with PCI DSS requirements for handling and processing payment card data?	
Are regular security audits conducted to ensure ongoing compliance and mitigate risks?	
Employee Awareness and Training	
Are employees trained in cybersecurity best practices, such as recognizing phishing emails and avoiding social engineering attacks?	
Is there a process in place to update employees regularly on emerging security threats and provide ongoing training?	
Incident Response and Recovery	
Is there an incident response plan in place to guide the organization in the event of a cybersecurity incident?	
Are incident response procedures regularly tested?	
Has the organization conducted tabletop exercises or simulations to test the effectiveness of the incident response plan?	

Questions	Score
Physical Security	
Are physical access controls implemented to prevent unauthorized entry to critical IT infrastructure areas?	
Are surveillance cameras and alarm systems used in critical areas?	
Vendor Management	
Are proper security measures in place when working with third-party vendors and partners with sensitive data access?	
Is there an assessment of vendor compliance with security standards?	
Are the performance and security practices of vendors monitored?	
Security Monitoring and Threat Intelligence	
Is network traffic and systems continuously monitored for anomalies?	
Are security patches and updates promptly applied to mitigate known vulnerabilities?	
Security Policies and Governance	
Is the organization compliant with relevant regulations and privacy laws?	
Are processes in place to monitor and address changes in regulatory requirements?	
Regular Security Assessments	
Are penetration testing and vulnerability assessments conducted regularly?	
Are security controls and processes audited regularly?	
Total Score:	

Very High Risk: 0-50

High Risk: 55–75

Moderate Risk: 80–100

Low Risk: 105–120