

# HOSPITALITY SECURITY PRACTICE OVERVIEW

The hospitality industry has undergone more digital transformation efforts in the last two years than in the previous two decades. Today, over **90% of critical business processes in the hospitality industry rely on interconnected digital networks**—for example, serverless infrastructures handle payment processing and guests' data storage.

Many hospitality businesses, such as hotels and restaurants, are retrofitted with smart entertainment systems with remote access portals that permit guests to log into existing streaming services and public Wi-Fi that is complimentary for all to use. However, **the more access guests have to connect to different networks, the wider the attack surface becomes for potential cyberattacks.**

## WHAT MAKES THE HOSPITALITY INDUSTRY LUCRATIVE TO CYBERCRIMINALS?

- Access to multiple guests' data, including personally identifiable information (PII) like full names, addresses, payment card details, and other private information.
- An influx of interconnected devices traversing throughout the network
- An increased email communication workflow (between customers and employees)
- Poor cybersecurity awareness within hospitality staff.
- An absence of proactive threat detection and response measures
- The constant introduction of new and emerging technologies

## SECURITY PROGRAM OFFERING

- [Security Risk Assessments](#)
- Security Architecture Reviews
- Vulnerability Assessments (Monthly Scanning Services)
- Internal & External Network Penetration Testing
- Application Penetration Testing
- [EU-GDPR](#) Privacy Gap & Readiness Engagements
- [Chief Security Officer as a Service](#) (CSOaaS)
- [PCI-DSS](#) Compliance Gap & Readiness Engagements

- [ISO 27001](#) Compliance Gap & Readiness Engagements
- SOC 2 Compliance Gap and Readiness Engagements
- Vendor Access Security Management
- Security Technology Selection & Enhancement
- [Phishing Training and Simulation Services](#) (Security Awareness Training)
- Cloud, Mobile, and Wireless Security Services
- Security Plan Development
- Disaster Recovery & Business Continuity Planning
- Email Encryption Services
- Endpoint Protection Services

## WHY CHOOSE US

At Goldsky, **we are strategically equipped with sector-specific cybersecurity experts** capable of stepping in and assessing security postures and recommending globally-accepted, tailored security solutions to help minimize cyber risks.

Our approach involves a thorough assessment of your computing infrastructure, including IT architecture, critical assets (technology, people, processes), business operations, and other operating environments, to **uncover vulnerable areas to malicious threat actors or regulatory compliance fines.**

As your cybersecurity partner, **our ultimate goal** is to constantly enhance your cyber resilience posture with our [proactive threat detection](#) and mitigation approach. We welcome your hospitality company to leverage our threat discovery and visibility capabilities to understand your threat level without disrupting daily business services.

