Hospitality Sector: CYBERSECURITY RISKS *(And How To Be Prepared)*

The hospitality sector is one of the most targeted industries, and recent updates to the industry have significantly increased its risk profile. The interconnected boom the industry has experienced through WiFi, Bluetooth, and other IoT devices has indeed improved the customer experience, but the lack of security measures to manage this boom is leaving the industry exposed.

Here's what the hospitality industry needs to know and how to protect itself.

WHY THE HIGH RISK?

Loads of PII

The hospitality industry doesn't just collect sensitive financial information such as credit card details and addresses; it also often gathers social security numbers, passport numbers, and even travel itineraries that can lead to credit card fraud and identity theft.

Insider threat risk

The hospitality industry experiences a high employee turnover rate, making it more likely that an untrained employee could fall for phishing or social engineering attacks. Malicious actors also have a larger pool of past employees to exploit or compromise.

High value targets

Nation-state and politically motivated attackers can target government officials and other high-ranking individuals through vulnerable hotels, putting the targets at risk and creating a reputational catastrophe for the compromised company.

COMMON ATTACKS

IoT Device Compromise

The number of IoT systems in hotels has exploded in recent years, including Smart TVs, virtual check-in kiosks, security cameras, PoS systems, and virtual doorknobs.

Supply chain/third-party attacks

Attackers can compromise several companies via a major hospitality chain, or they can exploit a third-party, such as a cleaning service staffing company or a booking partner, to reach their primary target.

Point of Sale malware

These attacks skim sensitive data and have led to the loss of millions of records over the last few decades.

Hotel WiFi

Attacks can spoof WiFi networks or intercept legitimate connections to target unsuspecting travelers or high-profile individuals and steal important information.

Loyalty program fraud

These attacks steal loyalty points and can even extend to stealing personal information from loyalty program members, potentially leading to identity theft attacks.

IN THE NEWS

IHG HOTELS & RESORTS

IHG suffers a two-day outage

This UK-based hotel chain operator was hit by an unauthorized user, impacting their systems and resulting in a multi-day outage that affected customers' ability to manage bookings and related online operations.

CROWN RESORTS

Crown Resorts suffers a data breach from a ransomware group in 2023

Australia's largest gambling and entertainment company was targeted with a zero-day vulnerability on its file-sharing service, leading to the theft of sensitive business data by the ransomware group responsible for the attack.

Loyalty program fraud increase 89% in a single year

The rise in this kind of attack has also contributed to an increase in account takeover attacks, new account fraud, transactional fraud, and policy abuse, all of which can impact revenue and reputation.

HACKED

Singapore's biggest data breach hits a hotel booking site

The personal data of 5.9 million people were leaked due to an attack on RedDoorz, a popular booking site for Singapore and other South Asian countries.

HOW THE HOSPITALITY INDUSTRY CAN BE PREPARED FOR CYBER RISKS

Conduct Risk Assessments

Perform risk assessments at least annually to identify vulnerabilities and areas of elevated risk, thereby meeting key cyber insurance requirements.

Invest in cyber insurance

Cyber insurance can help cover some of the significant costs associated with a compromise, enabling you to handle the financial consequences of a successful attack.

Leverage zero-trust

A zero-trust architecture requires constant verification of entities and users and is designed to minimize the risk of a compromised third-party, device, or employee from being able to access the most sensitive parts of a company.

Enable MFA

This is low-effort with a huge impact. MFA vastly improves account security, minimizing the risk of many account takeover attacks.

Focus on comprehensive security

Cybersecurity is most effective when approached with a layered strategy, often necessitating multiple protective solutions that safeguard emails, endpoints, accounts, and provide detection and response capabilities.

Find an Incident Response Provider

An incident response retainer can expedite recovery time in the event of an incident, reducing costs, preventing future attacks, and potentially mitigating regulatory issues stemming from a compromise.

Train your employees

Continuous security awareness training can increase employees' understanding of the tactics and attacks they may encounter, minimizing the risk of insider threats.

Work with a managed security program partner

A managed security partner functions like an outsourced cybersecurity department, offering 24/7 detection and response services, a comprehensive security tech stack, and connections to key cyber insurance and incident response partners.

To learn more about how we can help your organization,

Check out SolCyber

SolCyber

solcyber.com