GUIDE

Stay a step ahead of cybersecurity threats in hospitality

1,270

The average number of cyberattacks experienced weekly by organizations in hospitality, travel and recreation.[1]

33%

Increase in the average number of weekly attacks reported by hospitality organizations from 2023 to 2024.[4]

95,040

The number of vulnerabilities identified in publicly exposed hospitality systems.[7]

Pressure to modernize and keep up with technology trends makes hospitality a dynamic and fast-changing industry. It also means that businesses like hotels can be particularly vulnerable to cyberattacks.

Staying competitive as guests' expectations grow can stretch resource-constrained IT teams that are also responsible for cybersecurity. In recent years, networks at many organizations have expanded to support:

- Occupancy sensors to assist housekeeping.
- Smart HVAC systems to save energy costs.
- Connected room service trays to improve service.
- Biometrics to speed check-in and increase security.
- Smartphone apps that simplify room access.
- AI-powered analytics to improve profitability and service delivery.

Innovations like these have allowed hoteliers to achieve new levels of efficiency and guest personalization. At the same time, they can greatly expand the threat surface their organizations need to protect from unrelenting cyberthreats. In the summer of 2024, 82% of North American hotels were hit with cyberattacks.[2] Hospitality organizations are a regular target of cybercriminals that attempt to gain access to guests' personally identifiable information (PII), steal credit card data or disrupt operations. The threat has grown so large that, in one survey, cyberattacks and data breaches topped the list of organizational risks identified by hospitality leaders.[3]

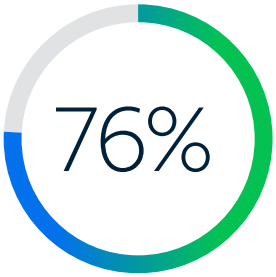
The cost of a cyberattack

The average cost of a data breach in the hospitality sector reached $4.03 million in 2025.[5] The damage isn't limited to repairing affected systems. Attacks that disrupt travel plans or expose guest information can also inflict long-lasting damage to brand reputation, erode consumer trust and increase legal liability.

Among hotel leaders, the top three impacts anticipated after a cyberattack are:[6]

1. Negative online reviews and reputational damage.
2. Major financial losses due to recovery costs.
3. Lawsuits and legal liabilities from affected guests.

To avoid these impacts, hospitality organizations must update their protection to match current threats while identifying vulnerabilities throughout their networks.



of hotel operators say enhancing data security is an important initiative.[8]

Tracking evolving threats

Protecting your organization requires an understanding of the most prevalent types of attacks. These include:

Social engineering

This technique is used by cybercriminals to exploit human psychology and trick people into revealing confidential information or performing actions that compromise security. Phishing is one common method, with attackers often impersonating legitimate entities to steal sensitive data or plant malware through malicious files or downloads.

AI-powered cyberthreats

These emerging methods leverage AI to create more convincing and automated attacks, making them harder to detect and potentially more effective. One example includes using AI to develop deepfakes, which are realistic fake videos, audio or images employed to trick individuals into granting access to systems or data. AI can also help generate highly personalized phishing emails, power chatbot phishing efforts and attack AI systems by corrupting training data or finding vulnerabilities in the models. Nearly half of hotel IT and cybersecurity leaders say they aren't confident in their ability to identify sophisticated AI-driven cyberattacks and deepfakes.[9]

Ransomware and other malware

Malware is broadly defined as any malicious software designed to harm or exploit computer systems. Ransomware is a type of malware attackers use to restrict access to a computer system or files and then demand payment for their release. Disrupting revenue at the most critical times of the year, ransomware attacks were the most common type of cybersecurity incident in the retail and hospitality industries during the 2023 holiday season.[10] Downloaders are another common malware type, distributed through malicious or compromised websites, typically via fake software updates. New malware variations appear each year, underscoring the need for organizations to remain up to date and vigilant.

Distributed denial of service (DDoS) attacks

These brute-force attacks are throwing more traffic at networks than ever before, combining volumetric, session-exhaustion and application-layer attack vectors. In session-exhaustion attacks, the firewall is essentially turned inside out, becoming a tool for attackers instead of a network defense. Application-layer attacks target the code that runs the website or application. The average cost of an application-layer DDoS attack is $6,130 per minute.[12]

Data breaches

The unauthorized access, disclosure or loss of sensitive, confidential or protected information continues to be a risk faced by hospitality organizations large and small. The theft can involve PII, such as Social Security numbers, bank account details and passport numbers, as well as confidential corporate data. In some cases, attackers prefer to corrupt rather than steal from databases: deleting tables, changing records or erasing entire databases.

Areas of vulnerability identified by hotel technology leaders:[11]

1. Payments and point-of-sale systems (72%).
2. Guest WiFi (56%).
3. Front desk systems (34%).
4. Internet of Things room devices (22%).
5. Booking engines or websites (16%).

A next-generation firewall is key to protect data, prevent intrusion and warn security personnel of network vulnerabilities.

How cyberattacks can be prevented

Breaking down the details of hospitality cybercrimes helps paint a clear picture of the threat. Read these hypothetical examples and see how hotels might have been better protected against an attack.

Guest records stolen via phishing

Type of breach: A remote-access trojan and a tool that sniffs out usernames and password combinations in system memory — often downloaded from a phishing email — were used to steal guest records from a guest reservation database. This attack went undetected for four years.

What was lost: Hundreds of millions of guest records were breached. Many included highly sensitive information, including credit card and passport numbers, mailing addresses, birth dates and reservation information. In addition to loss of revenue, the company incurred millions of dollars in expenses to address the data breach.

What might have mitigated or thwarted the attack: Use of anti-malware protection and a next-generation firewall may have prevented the attack. Encrypted data, both in transit and at rest, would have rendered all emails and other records unreadable. Use of multi-factor authentication (MFA), updated software and expert training for employees about current phishing methods could have deterred the attack.

Ransomware accesses customer database

Type of breach: An unsecured database containing guest records was hacked. Hackers demanded thousands of dollars in bitcoin in exchange for the files.

What was lost: Hundreds of thousands of records with detailed guest information including names, email addresses and phone numbers were accessed. The database was accessible to anyone for four days before the breach was discovered.

What might have mitigated or thwarted the attack: The use of antivirus software and a next-generation firewall, as well as content scanning and filtering to detect threats in advance, could have prevented the intrusion. MFA and segmented security zones within the network could have hindered bad actors from moving laterally if they gained access to one device, while endpoint security solutions could help protect individual devices connected to the network.

DDoS attack shuts down hotel site

Type of breach: The website for a chain of hotels experienced a DDoS attack.

What was lost: Visitors to the website were met with a message advising them to check their browser before proceeding. The website was overwhelmed with traffic from a DDoS attack and customer payment information was stolen while the attack was underway.

What might have mitigated or thwarted the attack: DDoS protection services could have blocked the offending IP address and prevented secondary attacks. Machine learning and AI might have identified anomalies in traffic flows, triggering targeted IP address cleansing. With the address blocked, clean traffic would be allowed to pass, which would have enabled sites and applications to continue operations. In addition, access to a cloud-based portal may have provided the real-time traffic visibility, insights, analytics and in-depth reporting needed to help avert the attack or limit its impact.

Finding the right protection for your hotel

Continuously keeping ahead of cybersecurity threats to your network requires comprehensive and coordinated coverage. A unified security approach integrated with your internet and network connectivity can help you eliminate vulnerabilities and expedite issue resolution. The approach should include firewalls, unified threat management (UTM) and DDoS protection. The support of a network services provider is also vital, including for cloud-based security services such as secure web gateways, cloud access security brokers, identity management and zero trust network access.

When it's time to evaluate a provider and its services, ask the following questions to help you find the best protection possible.

- How can you protect us from malware, phishing and other common cyberattacks?
- How do you identify and mitigate network threats? Can you scan our network for attacks and drain suspicious traffic?
- What protection do you provide against volumetric DDoS attacks?
- Do you have a means for enabling us to continue to work productively on unaffected parts of the network after a DDoS attack?
- Do you provide UTM? What protection does that provide?
- Can your firewall protect traffic across our various sites?
- Is a next-generation firewall part of what you offer? What does it provide?
- Do you have an integrated solution that includes firewall, UTM and internet service to simplify protection?
- Does your solution provide complete visibility across network components to make potential vulnerabilities easier to identify?
- Can you help implement a zero-trust network architecture with MFA, access management and cloud security for staff working on-site and remotely?
- How are you prepared to support our organization as our network needs change and cyberthreats evolve?
- How can you help offload day-to-day administration work from our IT team during and after implementation?
- What types of teams and experts will we have access to for support? Are they available 24/7/365?
- How will you ensure all of our WiFi sites are protected?

Comprehensive coverage and support

Widespread, coordinated network protection can keep you one step ahead of evolving cyberthreats in the hospitality sector. You can balance the needs for complexity in coverage and simplicity in operation by choosing managed security services. With the right partner, you're supported from design through implementation and provided with ongoing support. See how Spectrum Business® is uniquely qualified to protect your network.

Learn more

1. "The State of Cyber Security 2025," Check Point Research, 2025.
2. "Peak Season, Peak Risk: The 2025 State of Hospitality Cyber Report," VikingCloud, July 2025.
3. "Top Risks Facing Hospitality, Travel and Leisure Organizations," Aon, November 28, 2023.
4. "The State of Cyber Security 2025."
5. "Cost of a Data Breach Report 2025: The AI Oversight Gap," Ponemon Institute and IBM Security, July 2025.
6. "Peak Season, Peak Risk."
7. "2025 Trustwave Risk Radar Report: Hospitality Sector," Trustwave, 2025.
8. "2024 Lodging Technology Study: Digital Transformation & ROI," Hospitality Technology, 2024.
9. "Peak Season, Peak Risk."
10. "2024 Holiday Season Cyber Threat Trends," Retail & Hospitality Information Sharing and Analysis Center, November 2024.
11. "Peak Season, Peak Risk."
12. "Application Security in a Multi-Cloud World 2023," Radware, November 8, 2023.

Spectrum BUSINESS®