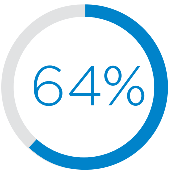
GUIDE

How to stay a step ahead of cybersecurity threats in hospitality

Spectrum ENTERPRISE

Pressure to modernize and keep up with technology trends makes hospitality a dynamic and fast-changing industry.



of hospitality data breaches occur in corporate internal networks.[6]

It also means that hotels are particularly vulnerable to network cyberattacks. The hospitality industry ranks third in likelihood of a data breach, just behind retail and finance.[1]

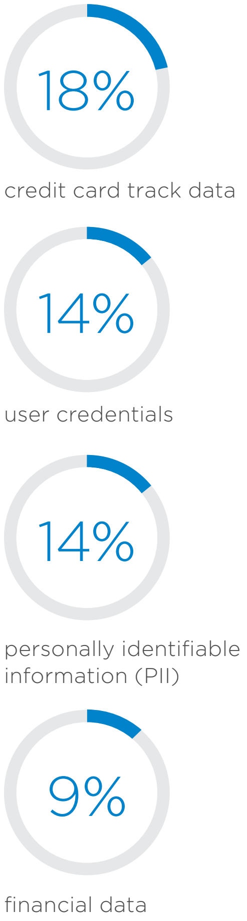
Currently, 50 percent of hospitality executives have active Internet of Things (IoT) projects,[2] such as occupancy sensors to facilitate room cleaning, smart HVAC systems to save money, connected room service trays to improve service, biometrics to speed check-in and increase security and many others. These innovations are important ways to improve and personalize the guest experience and manage costs. They also increase the number of security vulnerabilities. Add aging technology infrastructure into the mix, and it's no wonder hospitality is one of the most vulnerable industries.

Hotels are cyberattack targets because of the valuable customer data they collect. Credit card information, birth dates, passport numbers and other personal information is used by thieves to build profiles, which draw big interest — and huge money — on the dark web.

The threats targeting hotels are constantly evolving as hackers develop new tactics to gain entry to hospitality systems and develop workarounds to security responses. To fully understand the scope of threat, consider the numbers below:

- **64 percent** of hospitality data breaches occur in corporate internal networks.[3]
- **5.2 million** guest records were compromised in one hotel chain breach in 2020.[4]
- **137 percent** increase in cyberfraud attempts, making travel and leisure one of the most targeted industries in Q2 of 2021.[5]

Type of data cybercriminals target in hotels[12]



Tracking evolving threats

To protect your organization, you must understand the most prevalent types of attacks. The top three affecting hotels are:

- **Phishing:** Phishing attacks are growing in sophistication. Hackers today are targeting individuals in positions of authority — such as in payroll or accounts payable — with bogus emails in hopes of gaining access to the company's systems or convincing them to approve money transfers.
- **Ransomware:** Ransomware is a growing attack vector across all industries — hospitality included. In 2020, ransomware attacks increased by a shocking 435 percent over 2019.[7] Today, cybercriminals are not only encrypting data in these attacks, they're stealing it and threatening to release it on the internet.
- **DDoS:** The hospitality industry has become the top target for distributed denial of service (DDoS) attacks.[8] Volumetric DDoS assaults overwhelm networks to bring them down, while new attacks target group chats and send a barrage of malicious content rather than a sustained attack.

Hackers are launching these attacks through vulnerabilities in hotels' technology infrastructure. The most common points of entry include:

- **WiFi:** Hackers use "man-in-the-middle" attacks that appear as legitimate WiFi access portals to view their online activities, including online shopping and accessing bank accounts.
- **High staff turnover:** The hospitality industry has notoriously high turnover, making it a challenge to properly train staff on cybersecurity threats and protocols.
- **Point of sale (POS):** While POS attacks for many industries have decreased, they still represent a significant cybersecurity threat to the hotel industry, comprising nearly one-fifth of hotel cyberattacks in 2020.[9]
- **Third-party vendors:** As many as 80 percent of organizations report experiencing a cybersecurity breach originating from a vulnerability in their third-party vendor ecosystem.[10] Hotels partner with a vast number of vendors — such as payment processing systems and reservation applications — increasing opportunities for hackers to launch malicious attacks.

The cost of a cyberattack[11]

Loss of revenue

- 80 percent of consumers will defect from a business if their information is compromised in a breach.
- 52 percent of consumers say security is an important consideration when making a purchase.

Loss of reputation

- 85 percent tell others about their experience.

Loss of opportunity

- Only 20 percent of Americans will continue to be a guest of a hotel after a data breach.
- Millennials are the least likely to patronize a company after a data breach.

Real-world cyberattacks

Details of hospitality cybercrimes help paint a clear picture of the evolving threat. Read these examples, and see how hotels might have been better protected against an attack.

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

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 tens of millions of dollars in expenses to address the data breach.

What might have mitigated or thwarted the attack: A next-generation firewall could have helped block the attack and warned security personnel to act sooner. Intrusion detection services, in concert with strong client authentication, could have protected critical data.

Ransomware accesses customer database

Type of breach: An unsecured database containing customer 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 included names, email addresses and phone numbers. The database was accessible by anyone for four days before the breach was discovered.

How the breach could have been prevented: Anti-virus software and a next-generation firewall could have protected the data, prevented intrusion and warned security personnel of the vulnerability.

DDoS shuts down hotel site

Type of breach: The website for the 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.

How the breach could have been prevented: Monitoring could have caught the attack, while security help from a managed service provider (MSP) could have blocked the offending IP address and allowed clean traffic to pass through.

Finding the right protection for your hotel

Continually keeping ahead of cybersecurity threats to your network requires comprehensive and coordinated coverage. That includes firewalls, unified threat management (UTM), DDoS protection and the support of a network services provider to deliver managed service solutions.

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 hotel cyberattacks?
- What protection do you provide against volumetric DDoS attacks?
- Do you provide UTM? What protection does that provide?
- Can your firewall protect traffic between our various sites as well?
- 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?
- Threats are evolving, and our network is always changing and growing. Can you support us and our network investment as the environment and our needs change?
- We have a small technology staff. How can you offload day-to-day administrative work from our staff?
- What type of team and experts will we have access to for service?

Comprehensive coverage and support

Widespread, coordinated network protection coverage can keep you one step ahead of evolving and growing hotel network threats. When you choose security as a managed service, you are supported from design through implementation and thereafter. See how Spectrum Enterprise is uniquely qualified to protect your network.

Learn more

1. "2020 Trustwave Global Security Report," Trustwave, Jan. 2020.
2. Verma, Sanjeev, "Perks of Using IoT in the Hospitality Sector," Data Science Central, June 10, 2020.
3. "2020 Trustwave Global Security Report," Trustwave, Jan. 2020.
4. "Up to 5.2 million guests affected in Marriott breach," Hotel News Now, 2020.
5. "Fraudsters Shift Focus at Mid-Point of 2021 from Financial Services to Travel and Leisure and Other Industries," TransUnion, Aug. 11, 2021.
6. "2020 Trustwave Global Security Report," Trustwave, Jan. 2020.
7. "2020 Cyber Threat Report," Deep Instinct, 2020.
8. "Akamai 2020 State of the Internet/Security Report," Akamai, 2020.
9. "2020 Trustwave Global Security Report." Trustwave, Jan. 2020.
10. Gurinaviciute, Juta, "5 Biggest Cybersecurity Threats," Security Magazine, Feb. 3, 2021.
11. "Analyzing company reputation after a data breach," Varonis, 2020.
12. "2020 Trustwave Global Security Report," Trustwave, Jan. 2020.

About Spectrum Enterprise

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving many of America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions: Internet access, Ethernet access and networks, Voice and TV solutions. The Spectrum Enterprise team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs. For more information, visit enterprise.spectrum.com.

Not all products, pricing and services are available in all areas. Pricing and actual speeds may vary.
Restrictions may apply. Subject to change without notice.

Spectrum ENTERPRISE