Hotel Cybersecurity: How to Protect Your Property and Avoid Risks

Submitted by mtriquell@hote... on Thu, 09/10/2025 - 11:55

Some sectors are more vulnerable to cyberattacks than others, and the hospitality industry is one of them.

Due to the vast amount of personal and financial data it handles daily, combined with increasing digitalisation, **cybercriminals are seizing new opportunities** to attack this industry.

This landscape demands that **hotels improve their cybersecurity measures** not only to protect their guests but also to safeguard their business continuity.

This article will explore how cybersecurity is currently affecting the hospitality sector, as well as the **opinions of experts** in the field.

Cybersecurity threats to the hospitality industry: An overview

Cybersecurity is becoming an increasingly prominent topic—and for obvious reasons. By **2028**, global cybercrime damages are estimated to **hit $13.8 trillion annually**, a staggering increase from the $10.5 trillion expected in 2025, report Cybersecurity Ventures and Statista.

In hospitality, the impact will be especially evident: vulnerabilities in IoT and connected technologies are forecast to cost businesses **over $3 trillion worldwide by 2026**. This is particularly relevant as hotels increasingly adopt smart solutions like contactless check-in, automated services, and AI-powered guest experiences.

What does this mean? **Hotels will need to continuously strengthen their security measures** to protect both their guests and their business, as the associated costs—especially regarding reputation loss and customer trust—could soar.

In relation to this, **Scott Patterson**, CEO of The Knox Corps and an expert on **cybersecurity best practices**, points out that '*there are organisations that, if attacked today, would not survive tomorrow. A breach could lead to bankruptcy, and customers' financial and confidential information could be at risk.*' This brings us to the next section of this article.

Why is the hospitality industry particularly vulnerable to cyberattacks?

To begin with, as **Christo Butcher**, Global Lead for Threat Intelligence at NCC Group and Fox-IT, explains, '*the travel sector is particularly friendly, making its employees vulnerable to social engineering attacks.*'

The helpfulness of staff can become an entry point for cyberattacks. '*Additionally, cybersecurity levels in the hospitality industry are often lower than in other sectors*', Butcher adds.

Apart from these factors, there are other reasons why hotels are an attractive target for cybercriminals, including:

- **Sensitive personal data:** Hotels store large amounts of information, from passport numbers to credit card details, making this data a lucrative target.
- **Multiple entry points:** Regarding this point, Scott Patterson states that 'the many access points in this sector make it easier to become compromised. Between email communications, phone calls, third parties, partnerships, websites, and even payments, the travel industry makes itself a prime target for cybercrime.'
- **Third-party providers:** Hotels often rely on third-party service providers, whose security practices can introduce additional risks.
- **Employee turnover:** The high turnover rate in the hospitality sector can create gaps in cybersecurity training. This year, it's estimated that 70% of hotel staff will have access to sensitive data without continuous cybersecurity training, according to the World Economic Forum.
- **Interconnected systems:** The integration of property management systems (PMS) with other platforms increases complexity and attack potential.

Considering all this, the more knowledge we have about potential attacks, the better prepared the sector will be. This principle is also supported by **Paula Felstead**, our Chief Tech, Data and M&A Officer at HBX Group: '*In an increasingly interconnected world, it's essential to champion awareness and collaboration around cybersecurity, empowering everyone to not just react to threats but to proactively work together.*'

Common types of cyberattacks targeting hotels

There is no doubt that the hospitality industry faces many challenges when it comes to cybersecurity. This happens more often than we might think, and it’s important to talk about it to understand **what new threats for hotels exist**, what tactics cybercriminals are using, and most importantly, what solutions are effective.

As Christo Butcher points out, '*While companies may be reluctant to admit they’ve been victims of cyberattacks, sharing their experiences, especially the technical details of the attacks, with trusted authorities like Fox-IT and NCC Group is crucial. Anonymous reporting helps the travel sector build stronger defences by learning from collective experiences, rather than keeping mistakes to themselves.*'

Here are some of the biggest challenges in the hospitality industry when it comes to cybersecurity for hotels:

1. Social engineering & phishing

Social engineering exploits the hospitality sector's customer service mindset, manipulating situations to benefit cybercriminals at the expense of targeted businesses.

Social engineering exploits human psychology rather than technical vulnerabilities.

- **Email Phishing:** Deceptive emails designed to steal credentials.
- **Spear Phishing:** Attacks targeting specific individuals.
- **Voice Phishing (Vishing):** Fraudulent phone calls to extract confidential information.

Prevention:

- Regular staff training on phishing and suspicious communication.
- Strong spam filters and email validation.
- Enable **two-factor authentication (2FA)** on all critical systems.

2. Supply chain vulnerabilities

The integrations between hotel systems and external suppliers are frequently targeted in cyberattacks. A weak point in an **API** can compromise the entire network.

Prevention:

- Implement strict access control for third parties.
- Conduct regular audits of vendor cybersecurity policies.
- Use endpoint monitoring tools to detect anomalies.

3. Ransomware

This type of attack involves locking down critical systems until a ransom is paid. These attacks are **expected to rise significantly** in the coming years, especially if adequate security solutions are not implemented.

Prevention:

- Maintain secure, offline backups.
- Use advanced threat detection systems.
- Continuously educate teams on how to avoid suspicious links and downloads.

4. Internet of Things (IoT) attacks

The growing use of IoT devices in hotels, such as smart locks and climate control systems, increases vulnerabilities. Many IoT devices connect to the network **without robust security.**

Prevention:

- Ensure IoT devices use secure, unique passwords.
- Regularly update IoT device software.
- Encrypt data transmitted by IoT devices.

New & emerging cyber threats

Deepfakes & AI-generated attacks

Deepfake videos or audio generated by artificial intelligence can now convincingly impersonate a company executive or supplier—convincing staff to transfer money or share sensitive access credentials.

Prevention:

- Establish internal verification protocols for all high-risk requests.
- Train staff to be cautious, even when the “source” appears legitimate.
- Learn more about deepfakes via the **Spanish National Cybersecurity Institute**.

Identity theft & credential hijacking

Attackers are increasingly stealing staff or guest credentials, using them to gain persistent access to systems or resell on the dark web.

Prevention:

- Implement 2FA or multi-factor authentication across all systems.
- Monitor for abnormal login patterns.
- Encourage use of secure password managers.

New malware-based intrusions

Modern malware doesn't just aim to cause disruption—it seeks ongoing, hidden access. Attackers may try to steal your password, then install malware that quietly monitors activity long-term.

Prevention:

- Deploy endpoint detection and response (EDR) software.
- Limit administrative access to only essential users.
- Keep operating systems and software fully updated.

Practical cybersecurity tips for hoteliers

1. Change passwords regularly

Use long, complex passwords and rotate them every few months. **Avoid reusing passwords across systems**. A compromised password is often the first gateway to broader attacks.

2. Use two-factor authentication (2FA)

2FA adds an extra layer of protection, requiring not just a password but also a **verification code** sent to a separate device. It's a simple yet powerful way to block unauthorised access.

Many hospitality systems now support 2FA, and we strongly recommend all partners enable it. Our team can help walk you through this setup.

3. Run regular cyber risk assessments

Prevention starts with visibility. Tools like **Cybersential**, from our trusted partner Wallbid (and available for our hotel partners in **Europe and the UK**), give hoteliers a clear picture of vulnerabilities before they turn into costly breaches.

With a tailored cyber rating report and expert-reviewed action plan, you can:

- Safeguard guest data and protect your reputation.
- Prevent business interruptions from ransomware or data breaches.
- Save on recovery costs by addressing risks early.
- Ensure continuous security improvements with annual reassessments that track progress over time.

As an HBX Group partner, you can access Cybersential at an exclusive rate—making it easier for your property to identify risks, mitigate threats, and uncover hidden blind spots. Get in touch with Wallbid's team to learn more about the opportunities it brings to your property.

Final thoughts

The cybersecurity landscape for the hospitality industry in 2025 presents significant challenges, but also opportunities for those who are prepared.

The **evolution of digital threats**, especially with the rise of technologies like artificial intelligence and IoT, requires hotels to remain proactive in their defences.

As Scott Patterson mentions, 'Before focusing on trends, focus on the basics.' With a **solid strategy and a collaborative culture**, the hospitality industry can successfully face cybersecurity challenges ahead.

That's why we encourage you to invest time and effort in **learning more about the potential threats** your property can face, and **rely on partners committed to cybersecurity** that won't compromise your hotel, like HBX Group.

As Paula Felstead points out, '*At **HBX Group**, we see cybersecurity as a communal obligation. We all owe it not only to our own organisations, but also to every individual and business connected to us. Every transaction made within this ecosystem reflects our duty, and over the past three years, **we've faced emerging threats head-on by investing significantly in security**. With a dedicated cybersecurity team, we're committed to ensuring that every transaction is handled with care.*'

Are you interested in experiencing it firsthand? List your property today!

Register your property

Thumb image