knowbe4

Cyber Risk in Travel & Tourism EMEA 2026

Navigating Digital Transformation and Geopolitical Volatility in the EMEA Travel Sector

WWW.KNOWBE4.COM

KnowBe4, Inc. | 1 Leeds City Office Park, Meadow Lane, Leeds LS11 5BD
Tel: 01347 487512 | www.KnowBe4.com | Sales@KnowBe4.com

08680626

What's Inside

- 03 Risk in Travel & Tourism
- 04 Challenges
- 06 How Travel & Tourism is Being Attacked
- 08 State Of Cyber Attacks: Regional Case Studies
- 09 Regulatory Requirements
- 11 What Organisations Can Do: Addressing Human and AI Risk
- 12 Conclusion

Risk in Travel & Tourism

The Travel & Tourism industry in 2026 is no longer just a sector of leisure, recreation and business logistics; it has become a battlefield for cybercriminals and state-sponsored actors. It is a primary target for cybercriminals due to its high-volume handling of Personally Identifiable Information (PII) and its critical reliance on interconnected digital infrastructure.

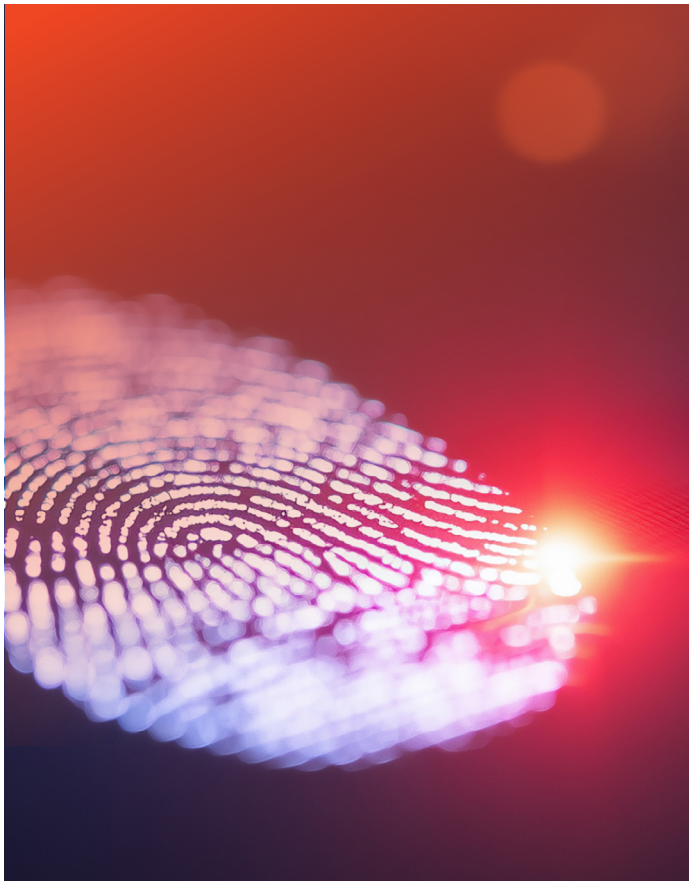
In Europe, the transport industry accounts for 11% of cyber attacks. It is the second most targeted, just behind the public sector (19% of cyber attacks).

The financial stakes have never been higher. According to the Ponemon Institute's Cost of a Data Breach Report, of those regions with the highest average cost of a data breach globally, EMEA regions accounted for three of the top five: the average cost of a data breach in the Middle East reached $7.29 million in 2025 , in Benelux they averaged $6.24 million while the United Kingdom saw average costs of $4.14 million per incident.

When it comes to industries, the average cost of a data breach in the hospitality industry was $4.03 million while in transportation it was $3.98 million.

These costs are not just driven by immediate remediation, but by the resale value of the stolen data, a high-value cocktail of passport numbers, credit card information and loyalty programme credentials.

Challenges



AI

The rapid rise of AI has thrown a fascinating paradox into the mix. On one hand, it is a powerful defensive tool, capable of detecting anomalies, automating responses, and processing threat intelligence at rapid speeds.

On the other hand, it is evolving into both a sophisticated means of attack and a valuable target. Cybercriminals use AI to create more convincing phishing emails, generate deepfake content for social engineering threats, and automate attacks at scale.

As the travel and tourism industry has fully embraced the 'Digital Guest Journey', from biometric check-ins to AI-curated itineraries, it has also inadvertently created a new and vast attack surface. Bad actors are wasting no time in developing new techniques specifically aimed at manipulating these AI systems. These include attacks such as prompt injection, model poisoning and adversarial inputs.

According to the World Economic Forum's Global Cybersecurity Outlook 2026, 94% of leaders now identify AI as the most significant driver of change in the threat landscape.

Geopolitical threats

Significantly, the travel industry has also been under extreme pressure due to geopolitical tensions across the globe. Ongoing conflicts have led to widespread fuel supply shortages and flight cancellations worldwide, which fundamentally reshape travel risk.

UN Tourism estimates that in a worst case scenario, international tourist arrivals in the Middle East could drop by 24% to 28% in 2026 (a loss of more than 24 million visitors) due to airspace closures and a plunge in traveller confidence. This disruption has led to a rise in attacks such as Global Navigation Satellite Systems (GNSS) jamming and 'spoofing'.

Phishing and social engineering

Phishing in the travel and tourism sector often exploits the high volume of communication between service providers and travellers. Attackers frequently use booking spoofing, where they create near-perfect replicas of popular hotel reservation sites or airline portals. A traveller, believing they are confirming a reservation, may enter their credit card details and passport information into a fraudulent interface.

According to KnowBe4's Phishing Threat Trends Report Volume Seven, 86% of Phishing Attacks are now AI-driven and there has been a seismic shift in the attack vectors used to conduct phishing attacks, including touchpoints outside of traditional email communication such as calendar invitations and messaging tools. In addition, more targeted social engineering was discovered, exemplified by internal team impersonation which was seen in 30% of attacks from threat actors in Q1 2026.

Ransomware

Ransomware groups use encryption to disrupt operations. This attack involves the encryption of critical data by malicious actors who then demand payment for the decryption key. In the context of a large hotel or resort, the encryption of a Property Management System (PMS) can lead to total operational paralysis; the staff cannot check guests in or out, access digital room keys, or process food and beverage charges. For airlines, ransomware can ground fleets by locking flight manifest systems or maintenance logs.

Over the last couple of years, the rise of Ransomware-as-a-Service (RaaS), a model where developers lease or sell ready-made ransomware tools, has made ransomware tools accessible to even inexperienced threat actors. By removing the need for advanced technical skills, it allows almost anyone to launch an attack, leading to a major spike in both the number and complexity of ransomware threats.

One of the modern trends observed is double extortion schemes. In these scenarios, attackers not only lock the systems but also exfiltrate sensitive traveller data, such as credit card and passport information, loyalty programme details and travel histories, threatening to release it publicly unless a ransom is paid. This is particularly damaging to luxury brands where guest privacy is a core part of the value proposition.

DDoS attacks

Distributed Denial of Service (DDoS) attacks aim to overwhelm a travel provider's digital infrastructure by flooding it with an unmanageable volume of automated traffic, rendering websites and mobile apps inaccessible to legitimate customers. In the highly competitive tourism market, where consumers often shop across multiple platforms simultaneously, even a few hours of downtime can result in massive revenue loss as travellers simply move to a competitor's site.

These attacks are frequently timed to coincide with peak booking periods, such as seasonal sales or major global event registrations, to maximise the pressure on the victim. Furthermore, DDoS attacks are often used as a tactical smoke screen. While the IT and security teams are occupied with restoring the website's public face, cybercriminals may simultaneously execute a quieter, more sophisticated breach of the internal databases to steal payment information or loyalty points.

Third-party risks

A significant challenge, unique to the travel and tourism sector, is the fragmentation of the supply chain. A single booking may involve a global distribution system (GDS), a third-party travel agency, a payment processor, and the final service provider, such as a boutique hotel or a local tour operator. Many smaller entities within this chain lack the large cybersecurity budgets of major international chains, making them a potentially weak link in the ecosystem.

An attacker may successfully breach a small regional tour operator and use their legitimate credentials to gain access to the broader network of a global partner. This interconnectedness means that a vulnerability in a single small hotel can potentially expose the data of thousands of travellers across the entire travel network.

Smart room tech

In upscale hotels and hospitality, digital assistants, smart TVs, and connected minibars have become commonplace. However, many of these devices suffer from insecure network configurations, out-of-date firmware or hard-coded credentials. These all have the potential to compromise the devices, which can leak guest data or provide a gateway for attackers to enter the wider hotel network or enable remote surveillance.

How Travel & Tourism is Being Attacked

Attackers are shifting away from brute-force breaking in towards highly-targeted, context-rich fraud using personalised, AI-powered social engineering.

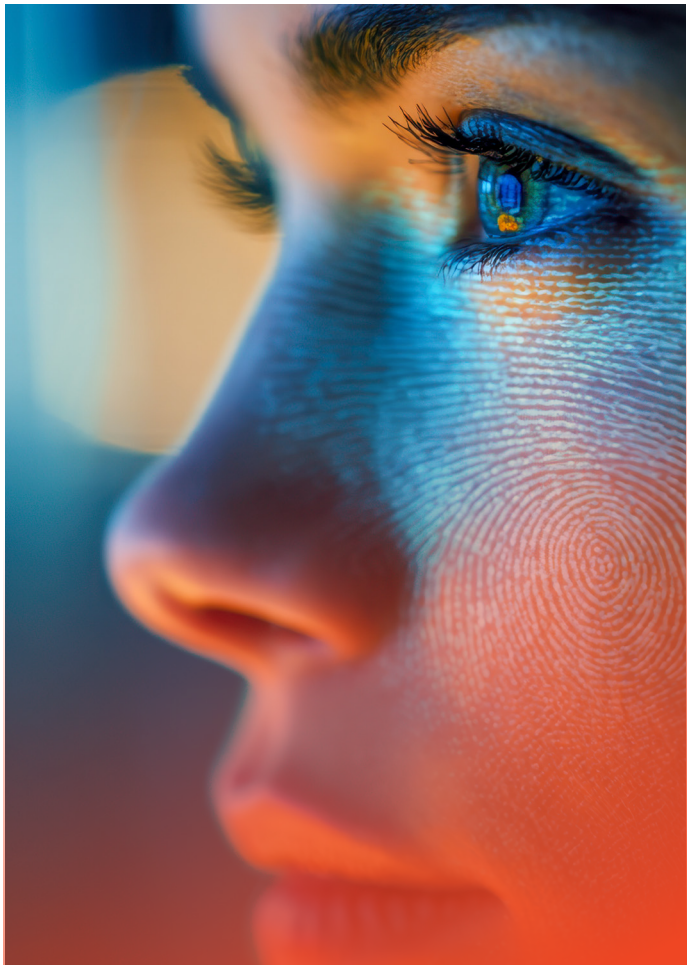
The reservation hijack

The most sophisticated example of modern travel fraud is the reservation hijacking campaign targeting a third party accommodation booking site. In early April 2026, threat actors compromised hotel partners across Europe using phishing techniques designed to trick staff into installing malware using a technique known as ClickFix - malware disguised as routine system fixes delivered via fake CAPTCHA pages.

Once inside, attackers hijacked the guest-hotel relationship. They sent messages to guests pretending to be hotels, referencing real booking numbers, dates and property names in order to trick victims into sending them money based on bogus reservation problems.

Supply chain strikes

The industry's reliance on centralised software is an Achilles' heel. In 2024, the Turkish-German airline, SunExpress, experienced a data breach impacting approximately 250,000 customers. The incident originated through a cyberattack on a third-party vendor responsible for handling its email newsletter distribution.



Attackers gained unauthorised access to roughly 596,000 email addresses stored by the external supplier, a database that included approximately 250,000 SunExpress customers. Following the breach, cybercriminals utilised the compromised data to launch targeted phishing campaigns, impersonating the airline to execute fraud and social engineering attacks against travellers.

Similarly, in March 2025, a major ransomware attack targeted Irec SAS, the French subsidiary of Vivaticket, a global online ticketing giant that manages roughly 850 million tickets annually across 50 countries. The breach was claimed by the RansomHouse cybercriminal syndicate, which successfully locked down systems and exfiltrated mass amounts of sensitive data.

The attackers claimed to have stolen extensive confidential documents and user data. Potentially compromised information included customer full

names, email addresses, purchase histories, reservation details, geographic locations, and account metadata (such as login timestamps). Approximately 3,500 European museums and monuments were paralyzed. French national landmarks, including the Louvre, and d'Orsay museums, Notre-Dame, the Arc de Triomphe, and the Eiffel Tower, lost access to secure online ticketing, forcing multiple venues to completely shut down online reservations and disrupting millions of travellers.

Check-in tech exposed

A security flaw in Ibis Budget self-check-in kiosks, identified in early 2024, exposed guest room keypad codes to potential hackers. By entering specific characters into the terminals, attackers could retrieve room numbers and corresponding door codes, allowing unauthorised access to rooms. The flaw affected self-service kiosks, primarily in Germany and across Europe, which allowed guests to check in without staff present. The vulnerability was addressed by Ibis Budget's parent company, French hospitality giant, Accor.

Ransomware groups attack critical infrastructure

In late 2025, the Russia-linked 'Everest' ransomware group claimed responsibility for the theft of 1.5 million passenger records from Dublin Airport and set a countdown timer demanding a $1 million ransom payment.

Hacktivists use DDoS

In 2024, the hacktivist group Anonymous Sudan claimed responsibility for a series of Distributed Denial-of-Service (DDoS) attacks against FlyDubai. The attacks, aimed at the UAE-based airline's systems including its website and online reservation systems, were reported as politically motivated, attempting to disrupt normal operations.

State of Cyber Attacks

United Kingdom

London Heathrow was severely impacted by a major aerospace ransomware attack in late 2025, resulting in thousands of cancelled flights. The UK also saw devastating attacks on major brands like M&S and Jaguar Land Rover in 2025. These attacks led to cybersecurity now being a board-level priority across the country.

France

In August 2025, Air France and KLM confirmed a data breach resulting from unauthorised access to a third-party customer service platform. Compromised data included names, email addresses, phone numbers, rewards programme information, and latest transactions, putting customers at risk of phishing.

BENELUX

In addition to the KLM breach (headquartered in the Netherlands), Belgium reported a 58% increase in cyber incidents in 2025 compared with the previous year.
The Centre for Cybersecurity Belgium reports it was among the European countries most frequently targeted by pro-Russian hacktivist groups with attacks often timed around geopolitical events.

DACH

The Lufthansa Group reported a data breach involving unauthorised access to passenger data handled by an external hotel voucher provider, in May 2025.
The breach exposed data such as names, gender, mobile numbers, flight details, and hotel reservation dates.

South Africa

South African Airways (SAA) experienced a significant cyber incident in May 2025 that disrupted its website, mobile app, and several internal operational systems.

UAE

The UAE faces a unique convergence of threats at the start of 2026.
The Cybersecurity Council reported fending off up to 200,000 attempted cyber breaches daily in the first couple of months of the year.

Regulatory Requirements

Regulators are no longer treating cyber risk as an IT issue. In the European Union, the NIS2 Directive now mandates strict risk management and reporting for essential sectors such as transport.

Businesses operating in tourism, particularly those offering digital services such as booking platforms, payment gateways, hotel chains, and online travel agencies, may also be affected if they meet the Directive's criteria. Criteria include medium and large enterprises (more than 50 employees or with a turnover exceeding €10 million), entities identified as essential or important, and companies critical in the provision of digital services, including those with reservation platforms or those managing sensitive data.

Non-compliance can lead to fines of up to €10 million or 2% of global turnover and, critically, Member State authorities have the power to hold individuals liable for breach of their duties to ensure compliance with NIS2. In certain circumstances, the competent authority could request the imposition of a temporary ban against a person at CEO or legal representative level in discharging managerial responsibilities.

NIS2 also impacts all entities that provide essential or important services to the European economy and society. Companies and suppliers that fit the specific categories are expected to comply with NIS2 when conducting business with European organisations, regardless of whether they are based within or outside of the EU. In addition, article 26 stipulates that organisations located outside of the European Union must appoint a representative in one of the EU member states where they offer services.

In the UK, the government is using the Cyber Security and Resilience (NIS) Bill to modernise its own regime and close the gap with the EU. The direction of travel is similar to NIS2. The Bill expands the scope of the UK regime to bring in new types of services and to give regulators power to designate critical suppliers.

In the Middle East, the introduction of the UAE National Cyber Security Strategy (2025-2031) has signaled the end of voluntary compliance and a move toward mandatory resilience. The strategy is structured around core pillars that define how the country protects its digital ecosystem, strengthens resilience, and enables secure innovation. These pillars guide execution across government entities, Dubai-based enterprises, and critical sectors.

However, cybersecurity compliance requirements in the UAE are not defined by one control set alone. They combine national laws, sector-specific regulations, government security controls, and technical obligations for organisations operating in the UAE.

Across Africa, the region has transitioned from an era of theoretical compliance to one of tangible enforcement. Regulatory bodies have stepped up their efforts as active enforcers; adjudicating disputes, levying fines and securing convictions.

In South Africa, the Information Regulator has also adopted a more assertive approach to POPIA enforcement, focusing specifically on high-impact sectors that hold large customer databases. Authorities are issuing significant financial penalties for non-compliance, as well as criminal convictions and prison sentences in South Africa for data offences.

What Organisations Can Do: Addressing AI and Human Risk

The travel and tourism industry is subjected to expensive, complex, and high-frequency cyber assaults. Given the growth of digital technology and greater dependence on external providers, the sector must stop depending on reactive responses. Establishing long-term resilience requires a unified approach that secures technology, agentic AI, and human elements.

1. Embed Cybersecurity into Digital Transformation

Cyber resilience must be embedded in all digital channels, including mobile booking apps, online platforms and AI-driven analytics:

- Implement cybersecurity-by-design for new apps, cloud services and data platforms.
- Conduct regular risk assessments across digital services and customer-facing applications.
- Align with NIS2, POPIA and other relevant regulatory frameworks.

2. Strengthen Third-Party and Supply Chain Oversight

The travel and tourism industry is highly dependent on external providers, meaning the risk of large-scale attacks is high:

- Maintain rigorous vendor risk management programmes for all third-party providers.
- Require security audits and resilience testing from critical suppliers.
- Include third parties in incident response planning and communication protocols.
- Share threat intelligence with trusted partners to anticipate emerging risks.

3. Secure the Digital Workforce

Even the most advanced firewalls cannot stop a breach if a human or an AI agent is tricked into giving access to the attacker. Organisations must shift their focus toward securing the digital workforce, which includes both humans and AI agents:

- Support employees by deploying intelligent anti-phishing systems to neutralise sophisticated attacks.
- Provide personalised, responsive and relevant security awareness training based on individual roles and departments.
- Run simulated phishing campaigns to improve detection and response.
- Offer just-in-time nudges to correct risky behaviour in real-time.
- Invest in cybersecurity talent and leadership, creating clear career pathways in IT and risk functions.
- Secure the AI agent workforce from threats such as prompt injections or ‘permission creep’, where an agent inadvertently accesses and exposes sensitive information.

While increased IT investments are great at strengthening defences against DDoS and other technical attacks, threats such as ransomware, phishing and third-party breaches require attention to processes, culture and behaviour to ensure true operational resilience.

Conclusion

The travel and tourism industry stands at a critical juncture in 2026. The digital transformation that has enabled global connectivity has also created a complex, AI-augmented attack surface.

While traditional security models have focused on securing the perimeter with technical controls, organisations must now turn their attention to securing the behaviour of the workforce. The booking platform hijack and supply chain disruptions prove that even the strongest perimeters can be bypassed when the human element is manipulated. Organisations must move beyond static annual training toward a continuous, real-time strategy to secure the digital workforce.

In 2026, the workforce is no longer just human employees; it includes AI agents embedded into critical workflows. Achieving true resilience requires visibility, accountability and security across both human and machine interactions. We must train humans to safely oversee AI agents and secure AI systems from adversarial manipulation.

The future of cybersecurity belongs to those who stop trying to lock people down and start designing systems that help them make better decisions at the critical moment.

By fostering a culture of high-trust and transparency, travel and tourism organisations can ensure that they remain secure and bridge the gap between digital vulnerability and sustainable growth.

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Email Exposure Check
Find out which of your users emails are exposed before bad actors do

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

About KnowBe4

KnowBe4 empowers the modern workforce to make smarter security decisions every day. Trusted by more than 70,000 organizations worldwide, KnowBe4 is the pioneer of digital workforce security, securing both AI agents and humans. The KnowBe4 Platform provides attack simulation and training, collaboration security, and agent security powered by AIDA (Artificial Intelligence Defense Agents) and a proprietary Risk Score. The platform leverages 15-years of behavioral data to combat advanced threats including social engineering, prompt injection, and shadow AI. By securing humans and agents, KnowBe4 leads the industry in workforce trust and defense.

More information at www.KnowBe4.com.

Follow us on Linkedin

Follow us on X

knowbe4

KnowBe4, Inc. | 1 Leeds City Office Park, Meadow Lane, Leeds LS11 5BD
Tel: 01347 487512 | www.KnowBe4.com | Sales@KnowBe4.com