SecureTrust™
BY VIKINGCLOUD®

REPORT

The Hottest Destination for Cyber Risk:

SecureTrust's 2026 Travel Agency Resilience Report

Executive Summary

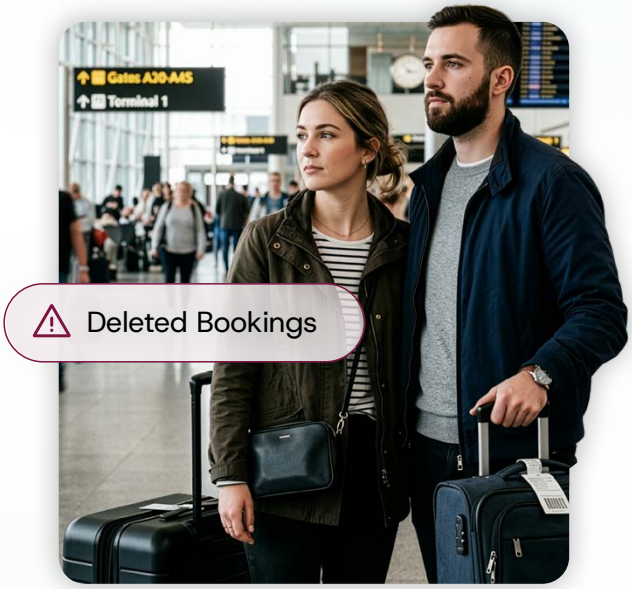
Travel agency owners identify cybersecurity as the single greatest threat to their business viability in 2026.

It's no surprise, given that **92% of agencies report experiencing cyber threats over the last 12 months**, with 66% of agencies having sensitive customer data compromised in that same period.

That ranking is notable because travel agencies are navigating enterprise-level risk with the resources of a small business. Inflation continues to affect margins, recession concerns threaten consumer spending, and geopolitical instability hinders traveler confidence. AI is changing how people research, plan, and book trips, and reshaping how agencies compete for customer loyalty. Even against that backdrop, cybersecurity tops the list.

To understand how small travel agencies are managing cyber risk, SecureTrust surveyed owners, operators, and cybersecurity leads across the U.S. and U.K.

The 2026 Travel Agency Resilience Report examines where agencies are most exposed, what those risks mean for travelers, and how agencies are working to prevent the next cyberattack from disrupting customer vacations.



SecureTrust BY VIKINGCLOUD

Cyber Risk Is the Top Threat for Travel Agencies

Despite inflation, recession concerns, and geopolitical instability, travel agencies are most concerned with a lurking threat invisible to customers: cybersecurity.

The Top 3 Risks Posing the Greatest Threat to Agency Success in 2026

1 ⚠
68%
Cyberattacks, data breaches, and ransomware.

2 $
60%
Inflation and rising costs.

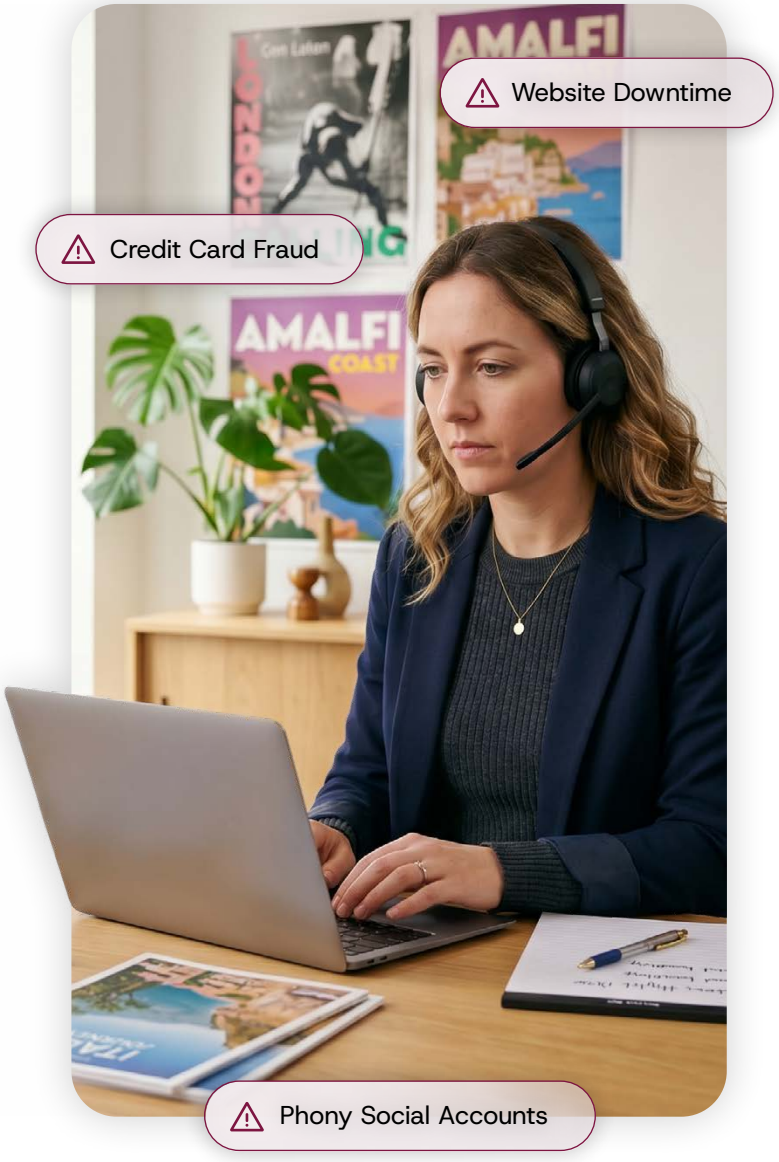
3 ↘
54%
Recession and reduced consumer spending.

Forces actively reshaping how travelers plan vacations fall further down the list, from rapid AI adoption by customers for booking travel (36%) to decreased international travel due to geopolitical tensions and safety concerns (20%). Operational challenges like workforce retention issues (20%) and hiring shortages (18%), as well as flight disruptions due to TSA or airline issues (18%), also rank lower.

Travel agencies' concern over cybersecurity is driven by experience: 92% of agencies reported experiencing cyber threats over the last 12 months. Phishing remains the primary threat, with 48% of agencies seeing employees or owners targeted by phishing texts or emails.

Other cyber incidents faced by travel agencies include website downtime (44%), fraudulent credit card activity (32%), phony social media accounts or fraudulent website domains (22%), ransomware (22%), and fake booking links (18%).

Alarmingly, 66% of travel agencies had sensitive customer information compromised over the past 12 months.



SecureTrust BY VIKINGCLOUD

Customer Data Exposed in Travel Agency Data Breaches

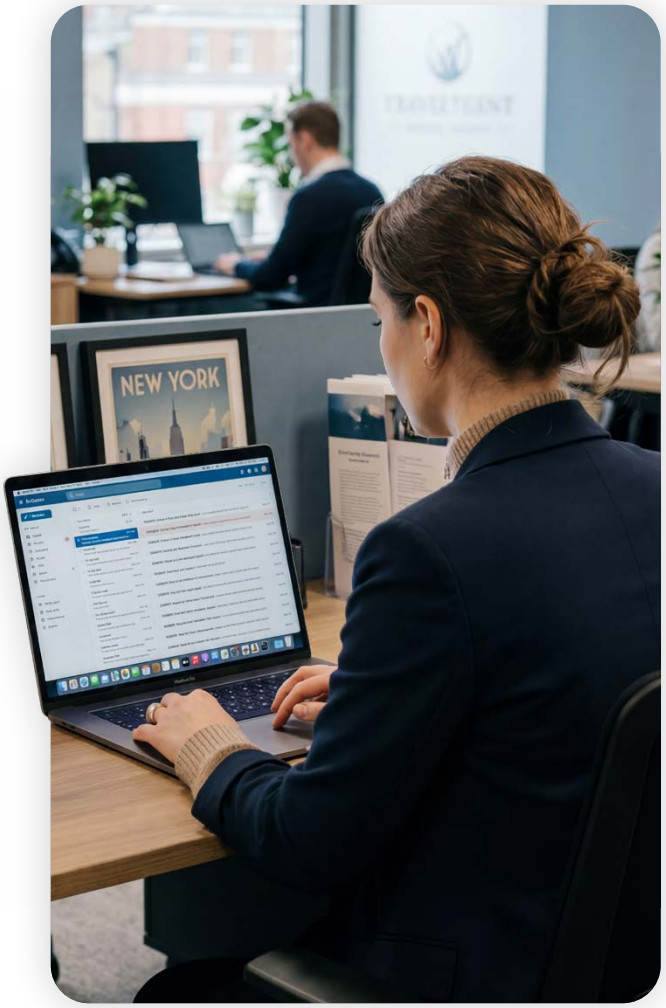
46% Phone numbers or emails

40% Personal details such as full names, date of birth, and home addresses

32% Credit card numbers

28% Passport details

22% Travel itineraries



Three Industry Realities Put Agencies at Risk

Travel agencies face a combination of operational vulnerabilities that make them attractive targets for hackers.

01 Fast-Paced Digital Operations Open the Door for AI-Savvy Attackers

AI is reshaping the threat landscape for travel agencies. Over a third (38%) of travel agencies faced AI-generated phishing or advanced "phishing-as-a-service" schemes in the last year. These automated attacks specifically exploit the high volume of itineraries and client contact moving through agency inboxes. In fact, 38% of travel agencies acknowledge that their heavy reliance on email communications makes them vulnerable to AI-powered phishing attacks.

Operational speed compounds the risk. 24% of agencies say the urgent nature of travel purchases leads them to bypass MFA or verification steps during peak hours, such as holiday rushes or major flight disruptions, to avoid losing a sale. Each shortcut creates an opening that attackers are increasingly capable of finding and exploiting at scale.

Without consistent security awareness training, clear policies, and the discipline to maintain them even during peak periods, agencies hand attackers the operational gaps they need.

02 Third-Party Vendor Operations Create Invisible Entry Points

Travel agencies manage a complex web of external integrations with limited visibility. More than half (56%) of agencies are only somewhat confident in the security of their booking systems, APIs, and payment processors, with most relying on periodic reviews rather than continuous monitoring to vet these partners.

Vendor reliability is a persistent issue. 28% of travel agencies faced a third-party or vendor outage in the past 12 months. Yet, despite these disruptions, 14% of agencies do not monitor the security posture of any of their third-party vendors.

The threat surface across third-party agency operations is huge for a small business. The third-party vendor operations presenting the greatest risk for a cyberattack in the next 12 months include:

56%
Payment processing gateways

52%
Cloud-based booking and global distribution systems

42%
Identity & document verification services

30%
Airline and hotel APIs

Just one vendor breach could impact the entire network, exposing sensitive customer information, disrupting revenue collection, and halting all vacation bookings.

03 Payment Security Is Evolving Faster Than Traditional Defenses

In the past 12 months, travel agencies reported fraudulent credit card activity (32%), credit card skimming (16%), and POS software downtime (14%) as their top payment risks.

But while these traditional payment channels remain under attack, they are no longer the industry's only concern. The way customers pay is changing as tokenization, biometrics, and new digital wallets move from novelty to norm, and attacker tactics evolve to capitalize on these new payment methods.

The Immediate Payment Security Gap

52% **of agencies acknowledge new payment methods will have a significant or extreme impact on their security risk, and 8% have already had biometric or tokenized payment details compromised in a data breach over the past 12 months. The threat isn't on the horizon. It's here.**

Awareness of these risks is significant, with 52% admitting that evolving payment methods will significantly or extremely impact their security risk.

This convergence of AI-driven attacks, complex vendor webs, and shifting payment methods has created a sophisticated threat landscape that few small agencies are prepared to navigate. Despite the rising stakes, the responsibility for defending this territory often falls on a single, non-technical point of failure: the owner.

The Owner-as-IT-Lead Blind Spot

44% of agency owners report they manage cybersecurity entirely on their own. 26% admit that they, or the person managing their cybersecurity, don't have sufficient training to do the job.

This expertise gap results in a breakdown of basic cyber hygiene and prevents agencies from identifying and investing in the modern tools and training required to keep pace with today's threat landscape.

For example, 40% of travel agencies admit their credentials may have been exposed or reused, while 28% report that employees share passwords across multiple systems. Another 36% of agencies say their cybersecurity technology is outdated; 12% can't keep up with software patches or updates.

When these vulnerabilities are exploited by cybercriminals, many agencies are left without a roadmap for recovery. Only 20% of travel agencies plan to develop an incident response plan over the next 12 months.

Business Risks Are High, With Direct Impacts on Traveler Experiences

The cost of a cyberattack extends far beyond immediate financial loss. Disruption quickly becomes visible to the customer, turning a security failure into a service disruption. In an industry defined by thin margins and seasonal surges, even a single disrupted booking window can be detrimental to revenue and reputation alike.

In fact, nearly half of agencies (46%) say a financial loss of less than $100,000 would begin to affect their ability to deliver an acceptable customer experience.

Beyond financial concerns, travel agencies' reputations are on the line. Agency leaders rank several "worst-case" scenarios where the reputational fallout would be permanent, including:

54%

A long-term client learning that their passport scans and visa documents have been posted to the dark web, exposing them to lifelong identity theft risk.

48%

Customers arriving at the terminal to find bookings deleted or itineraries altered by a hacker, leaving travelers stranded without support.

28%

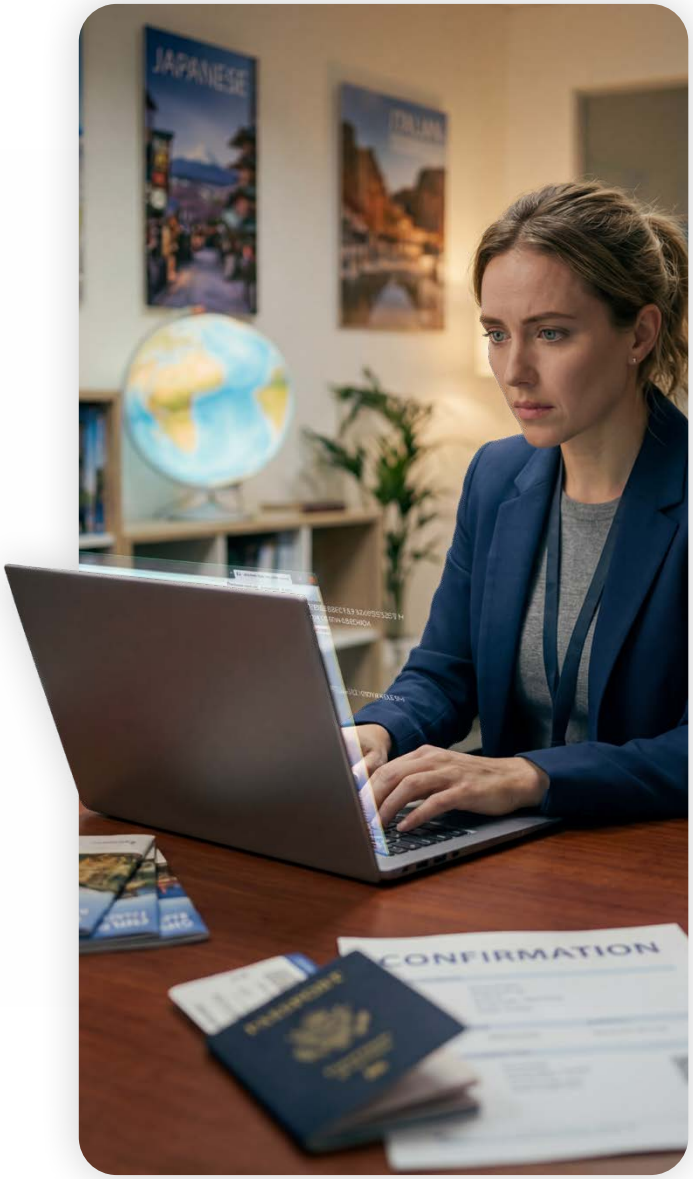
A full system outage that leaves staff unable to access booking tools or answer phones while customers are managing an active travel emergency.

26%

Customers losing years of accumulated travel points after loyalty-account credentials are stolen from an agency database.

22%

Stolen itineraries allowing criminals to track travelers and target their homes for robbery while they are away.



SecureTrust BY VIKINGCLOUD

How Agencies Are Responding Today

Travel agencies understand the stakes, and most are focused on strengthening the basics. Top steps agencies plan to take over the next 12 months to protect their business include (1) improving password security (56%) and (2) adopting cyber fundamentals like MFA or security awareness training (52%).

Beyond the basics, agencies are exploring additional layers of protection:

50%
plan to use automation or AI tools to improve threat detection and response.

36%
plan to implement a more rigorous cybersecurity standard for all third-party vendors.

26%
plan to apply end-to-end data encryption.

Each of these has merit, but most require significant investment, internal expertise, or new headcount.

For the majority of small travel agencies, the most accessible and impactful first step is a structured, supported approach to the fundamentals already required of them:

PCI Compliance.

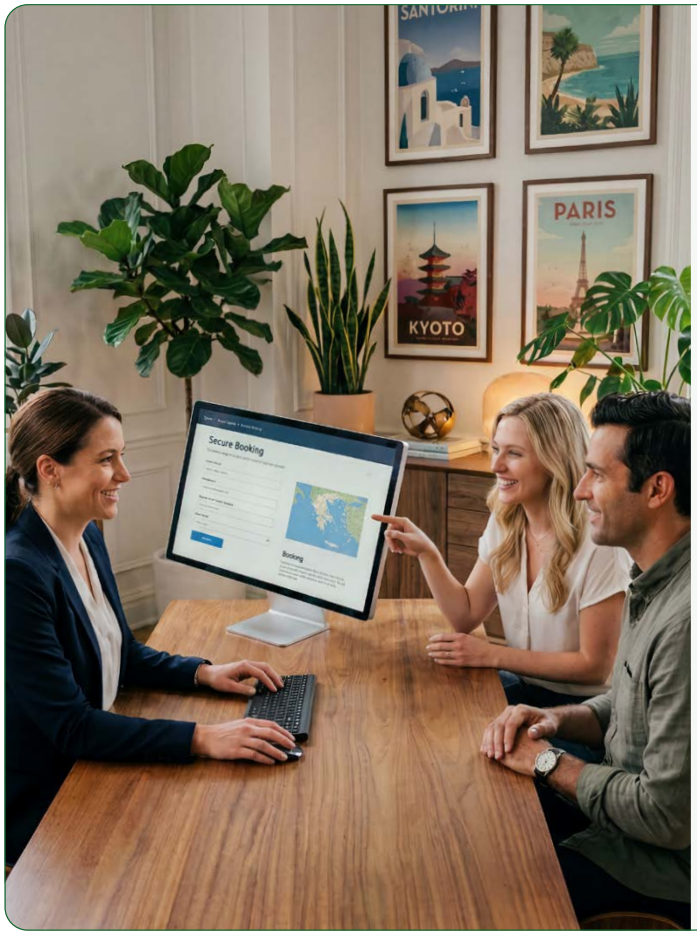
Three Steps Travel Agency Leaders Should Take to Address Their Cyber Risks

1. **Make PCI Compliance Easier, Not Harder:** PCI DSS v4.0 raises the bar with continuous security requirements, stricter multi-factor authentication, and formalized documentation. For small travel agencies handling card data across phone, email, and online bookings, navigating these requirements alone is a heavy lift. A guided PCI compliance program built for travel agents and advisors, complete with a step-by-step self-assessment, vulnerability scans, and security policy templates, turns mandatory annual compliance from a burden into a manageable, supported process.

2 **Get Visibility Into Vendor and System Risk:** Travel agencies depend on a complex web of booking platforms, payment processors, websites, and connected devices. Most rely on periodic check-ins to vet these partners, leaving exposure invisible between reviews. Regular vulnerability scans across the systems handling cardholder data give agencies continuous visibility into where their actual risk lives.

3 **The Owner Shouldn't Have to Be the Security Expert:** With 44% of agency owners managing cybersecurity themselves and 26% admitting they lack the training to do it well, the gap is human, not just technical. The right PCI compliance program meets owners where they are, with plain-language guidance, built-in education, and a clear path forward, so protecting customer data doesn't fall on someone forced to learn cybersecurity on the fly.

The travel industry has always thrived on its ability to navigate complex logistics and unpredictable environments. Today, that expertise must extend to the digital realm. The agencies best positioned for the year ahead will be those that treat compliance not as an annual checkbox, but as a continuous, supported function built into how they do business. In 2026 and beyond, the ultimate competitive advantage won't just be the best itinerary. It will be the demonstrable safety of the traveler's journey and the data behind it.



Built for IATA & Independent Travel Agents

SecureTrust PCI Manager is designed for the way IATA-accredited agents or small travel advisors handle card data across phone, email, and online bookings. Guided self-assessments, vulnerability scanning, security policy templates, and security awareness training help agencies meet PCI DSS requirements while minimizing operational burden.

Trusted by thousands of agents across 116 countries.

Learn more:
www.securetrust.com/industries/travel

SecureTrust™
BY VIKINGCLOUD®

The Hottest Destination for Cyber Risk:

SecureTrust's 2026 Travel Agency Resilience Report

About this Survey

These findings are based on an April 2026 SecureTrust online survey of 50 travel agency owners, operators, and cybersecurity/IT leads at smaller agencies in the United States and the United Kingdom, managed by an independent market research agency.

About SecureTrust, a VikingCloud Company

SecureTrust, a VikingCloud company, simplifies PCI DSS compliance for small businesses through SecureTrust PCI Manager—a guided self-assessment tool with ASV-certified scanning and expert support designed for merchants without a dedicated IT security team. For more information on SecureTrust, visit www.securetrust.com.

VikingCloud delivers battle-tested cybersecurity and compliance protection that simply works. Our expert-led approach combines proven technology and AI-driven insights with dedicated support—keeping businesses secure, audit-ready, and uninterrupted.

VikingCloud is trusted by over 4 million businesses in 70+ countries to stop threats before they stop business, so they can work on what matters most. For more information, visit www.vikingcloud.com and follow us at www.linkedin.com/company/vikingcloud/.