Cyber risk resilience quarterly : threat intelligence for hotel, restaurants and tourism sectors. Q2 2026

UNIVERSITY OF WEST LONDON
The Career University

CYBER RISK & RESILIENCE QUARTERLY

Threat Intelligence for Hotel, Restaurant and Tourism Sectors

Q2 2026

ICHARM
International Center for Hotel and Aviation Resilience Management

Welcome from the Dean

James Edmunds
Dean, London Geller College of Hospitality & Tourism

Welcome to the second edition of the Cyber Risk and Resilience Quarterly. This edition covers incidents affecting hotel groups, restaurant and food service operators, tourism businesses, and their technology suppliers between April and June 2026. The report draws on regulatory filings, dark web disclosures, threat intelligence feeds, and vendor advisories. and documents twenty incidents, along with two attacks from the first quarter that only reached public notification during this period.

What is different this quarter from the last is where the vulnerabilities lay. Very few of these attacks originated from inside the organisations that bore the consequences. Instead, the cybercriminals gained access to guest records through cloud platforms operated by third parties, through booking software shared across hundreds of properties, and through storage that a supplier had left accessible by misconfiguration. The first quarter was defined by stolen credentials and operational disruption. This quarter was defined by data held beyond the firewall and, remarkably, no payment terminal or ticketing system anywhere in the sector was taken offline as it happened in the first quarter.

The sections that follow examine each incident in turn, explore the methods used, identify the groups responsible, and conclude with actionable recommendations for managers and security teams.

A Note from the Researcher

In the first quarter the weak point was identity. In the second it was the platform. Carnival Corporation lost approximately 8.7 million records because an employee granted access to somebody who asked for it, and every authentication control worked correctly throughout.

More than one hundred hotels across three countries lost reservation data through a flaw in booking software none of them controlled. Hotelogix and Treebo lost guest folios because cloud storage permitted access, so no intrusion took place at all.

Two further patterns deserve attention this quarter: the speed of extortion and the number of unverified claims. Stolen reservation data now reaches guests within days, and criminals were demanding money from Booking.com customers while the company was still in the process of notifying them. Then, eleven of the twenty incidents recorded here are based solely on a criminal group's claim of a breach, without independent verification nor statement from the affected organisation. Ransomware groups spent the quarter competing through the volume of victims they listed. This makes it difficult to know what is real and what is exaggerated or false.

We hope the information in this report helps managers and cybersecurity teams protect their organisations against these methods.

Prof. Alexandros Paraskevas
Chair in Hospitality Management & Director, ICHARM

Contents

Executive Summary

The hospitality and tourism (H&T) sector and their technology providers faced a high number of cyberattacks during the second quarter of 2026. This report records twenty confirmed and claimed incidents plus two from the first quarter that became public during this period. The information comes from regulatory filings, dark web disclosures, threat intelligence feeds and vendor advisories. Check Point Research recorded an average of 2,291 weekly cyberattacks per organisation in hospitality, travel and recreation during May 2026. This is a rise of 24% year-on-year, against a global all-industry rise of 2%.

Three attack patterns stood out: ShinyHunters used social engineering to reach cloud customer relationship platforms at Carnival Corporation, Aman Resorts and 7-Eleven within a single fortnight in April. These were the largest breaches of the quarter. Ransomware groups, mainly Qilin and DragonForce, stole data and threatened to publish it unless victims paid. Ten of the twenty incidents fell into this category. A phishing campaign against front-office staff at hotels across Europe and Asia ran from April onwards, was disclosed by Microsoft Threat Intelligence on 25 June under the name authentication laundering and remains active. No individual property has been named, and no group has claimed the campaign.

Five named threat groups carried out attacks during the quarter: This is fewer than the eleven recorded in Q1 2026. Qilin listed eight sector victims and ShinyHunters three, which means that the two groups account for eleven of the fourteen attributed incidents. Six incidents have no known attacker, including the Booking.com breach, the BWH Hotels intrusion and the hotel phishing campaign. Eleven of the twenty incidents are based on a criminal claim with no independent verification and no victim statement. Leak site listing dates should never be read as the date of the intrusion.

Six trends shape the current threat landscape:

- Phishing now comes through legitimate services that pass every authentication check because the sending domain is genuine.
- Attackers talk their way into cloud platforms instead of breaking through perimeter defences.
- Stolen reservation data is turned into fraud against guests within days.
- Malware runs in memory and writes nothing to disk, which defeats file-based detection.
- Misconfigured cloud storage has become a breach type that requires no intrusion.
- Leak site volume reflects competition between criminal groups, not the number of organisations actually compromised.

The methods observed during Q2 2026 give a clear picture of the attack vectors for hotels, restaurants and tourism businesses. These include phishing through trusted notification systems, memory-based malware on front-desk terminals, compromise of Salesforce environments through employee manipulation, pay-or-leak extortion with deadlines, exposure of third-party vendor credentials, bulk scraping of misconfigured cloud storage, web application flaws that allow long-term access, failures in shared booking software, and fraud against guests using stolen reservation records.

Risk varies by subsector:

- Hotels lost data through systems they did not operate. BWH Hotels had an intruder for six months. More than one hundred properties across three countries were exposed by a single flaw in shared booking software. Front-desk workstations were named by Microsoft Threat Intelligence as a specific target.
- Restaurant and food service operators accounted for eight of the twenty incidents and the sharpest rise in claimed ransomware attacks, at 80% month-on-month according to Comparitech.
- Tourism and travel organisations lost the data carrying the heaviest regulatory weight. Carnival Corporation, the cruise operator, confirmed approximately 8.7 million records tied to the Holland America

Mariner Society loyalty programme, covering names, dates of birth, gender, passport numbers and loyalty status. Detection came on 14 April and the breach notice followed on 27 May. More than 800,000 residents of Texas were notified under that state filing alone, and the full notified population has not been disclosed.

Attackers monetised breaches through two models that did not appear in the previous quarter:

- Extortion without encryption was used on data held in cloud platforms. Aman Resorts was given a deadline of 21 April and no systems were locked.
- Extortion without intrusion followed the discovery of misconfigured cloud storage at Hotelogix and Treebo. A ransom demand of 500,000 US dollars was attached. That is the only ransom demand disclosed against a sector organisation during the quarter. No payment or refusal was made public anywhere in the sector.

Legal exposure widened considerably, even though no claim had yet been filed. No class action from a Q2 2026 incident had been lodged at the time of writing. No regulator had announced an investigation. This reflects the timing of disclosures, not any reduction in exposure. The incidents span the Netherlands, Belgium, Ireland, Switzerland, Germany, Austria, France, Turkey, Thailand, Singapore, India, Australia and the United States. A single failure in shared booking software creates parallel obligations to three European supervisory authorities (Autoriteit Persoonsgegevens in the Netherlands, the Autorité de protection des données, in Belgium, and the Data Protection Commission in Ireland) at once. Detection and notification dates will be the first two facts examined in any claim, and both are established by the organisation's own records.

The recommendations in this report follow the control failures and exposure patterns seen in Q2 2026. They cover identity governance and visibility inside cloud platforms, behavioural and network monitoring for malware that leaves no file behind, phishing and authentication countermeasures for messages coming from trusted services, external exposure and cloud configuration auditing, and five tabletop exercise scenarios drawn from the incidents documented here.

1. Incident Chronology

The second quarter of 2026 saw a concentrated and geographically spread wave of attacks on hotel groups, restaurant and food service operators, tourism businesses and the technology providers that serve them. This chronology covers confirmed breaches, disputed claims and active campaigns. Attacks that happened during the first quarter but became public in Q2 are listed at the bottom of the table.

The information comes from regulatory filings, dark web disclosures, threat intelligence feeds and vendor advisories. Where a threat actor claim has not been independently confirmed, the report notes this. For every leak site listing recorded here, the date shown is the date the victim appeared on the site, not the date of the intrusion and, in most cases, the actual breach will have happened several weeks earlier. Analysts should check regulatory filings and victim statements before treating any of this material as settled fact.

Most of the attacks this quarter fell into three main patterns

- Identity-based attacks against cloud customer relationship platforms caused the biggest single-brand breaches. ShinyHunters ran a pay-or-leak campaign against Salesforce environments that hit Carnival Corporation, Aman Resorts and 7-Eleven within days of each other in mid-April.
- Ransomware with data theft produced the most disclosed incidents. Qilin was responsible for the largest share of sector claims, mostly in food service during June.
- A phishing campaign against hotel front-office workstations ran from April. Microsoft disclosed it on 25 June under the name authentication laundering. That campaign is still active and is the main live threat for this edition.

1.1 Incident Timeline

Date	Organisation	Threat Actor	Attack Vector	Impact / Data	Sub-sector
April 2026					
Early Apr	Booking.com (NL)	Unattributed	Unauthorised third-party access to reservation data	Guest names, email addresses, telephone numbers, home addresses, booking dates and free-text notes to hotels. Data reused at once in payment-redirection phishing	Tourism & Travel
14 Apr	Carnival Corporation (USA)	ShinyHunters	Social engineering of an employee, giving access to part of the IT estate	8.7 million records with 7.5 million unique email addresses. Names, dates of birth, passport numbers, loyalty status. Confirmed 27 May	Tourism & Travel
18/19 Apr	Aman Resorts (CH)	ShinyHunters	Salesforce environment compromise, pay-or-leak extortion	More than 500,000 records claimed, holding personal data. Ransom deadline of 21 April	Hotel
22 Apr	BWH Hotels (Best Western, WorldHotels, Sure Hotels)	Unattributed	Flaw in a web application holding guest reservation data	Guest names, contact details, reservation numbers, dates of stay and special requests. Access ran from 14 October 2025. Disclosed 11 May	Hotel
29 Apr	Ryanair (IE)	Unattributed forum actor	Data offered for sale on a hacker forum	Alleged legal claims platform data covering EU Regulation 261/2004 cases, internal correspondence, flight data, banking details	Tourism & Travel
Apr (unspec.)	7-Eleven	ShinyHunters	Salesforce environment compromise, pay-or-leak extortion	Named on the 18 April pay-or-leak warning list alongside Aman Resorts. Data categories not detailed	Restaurant & Food Service

Date	Organisation	Threat Actor	Attack Vector	Impact / Data	Sub-sector
Apr (unspec.)	Alsea (Domino's, Starbucks, Vips operator, LatAm)	Unattributed	Third-party technology vendor compromise	12.6 GB vendor exposure including plaintext credentials, transaction records, audit reports and live surveillance camera access	Restaurant & Food Service
Apr onward	Hotels across Europe and Asia (multiple, unnamed)	Unattributed	Phishing routed through Calendly notification infrastructure, delivering a memory-only Node.js implant	Front-office workstations compromised, reaching property management, payment and reservation systems. Beaconing over non-standard ports. Microsoft disclosure 25 June	Hotel
Apr / May	Hotelogix and Treebo Hotels (SG/IN)	shadowbyt3$	Misconfigured cloud storage permitting bulk scraping	Guest folios, contact details, arrival and departure dates, room numbers, partial card and transaction data. USD 500,000 demand	Sector Technology
Apr / May	Gelatissimo (AU)	DragonForce	Ransomware with exfiltration	352 GB claimed. Sample files covering employee records, financial information and internal documents	Restaurant & Food Service
May 2026					
Early May	Sysco (USA)	Qilin	Ransomware and data extortion	Leak site listing with screenshots of alleged internal documents. Negotiation deadline of 12 May. No operational impact disclosed	Restaurant & Food Service
15 May	Australian hospitality and gaming IT supplier	Qilin	Ransomware	Listed on the Qilin leak site. Downstream hospitality and gaming customers potentially exposed	Sector Technology
May (unspec.)	Mopaş Online Supermarket (TR)	AUDIT TEAM	Ransomware and leak site extortion	Breach of systems confirmed by the company after the listing appeared	Restaurant & Food Service
June 2026					
Early Jun	More than 100 hotels (NL/BE/IE)	Unattributed	Probable vulnerability in shared hotel booking software	Customer and reservation data stolen and reused in phishing messages demanding payment under threat of cancellation	Hotel
2 to 5 Jun	Jay's Catering (USA)	Qilin	Ransomware	Leak site listing during the June claim spree. Data categories not disclosed	Restaurant & Food Service
2 to 5 Jun	Don Don Group	Qilin	Ransomware	Leak site listing during the June claim spree. Data categories not disclosed	Restaurant & Food Service
2 to 5 Jun	InterSPA-Gruppe (DE)	Qilin	Ransomware	Leak site listing during the June claim spree. Data categories not disclosed	Tourism & Travel
3 Jun	Eat Salad (FR)	Qilin	Ransomware and data extortion	Threat to publish unless negotiations commence. Data volume and categories under investigation	Restaurant & Food Service
4 Jun	Avcon Jet (AT)	Qilin	Ransomware and data extortion	Sensitive data samples posted to the Qilin leak site on 4 June	Tourism & Travel
21 Jun	Sivatel Bangkok (TH)	Qilin	Ransomware and data extortion	Threat to publish sensitive data unless negotiations commence	Hotel

Date	Organisation	Threat Actor	Attack Vector	Impact / Data	Sub-sector
Q1 2026 Attacks Disclosed During Q2 2026					
Mar 2026	Taos Mountain Casino (USA)	DragonForce	Ransomware with exfiltration	Names, addresses and Social Security numbers. 38.6 GB claimed. Notifications issued during Q2	Tourism & Travel
Mar 2026	RCI Internet Services (USA)	Unattributed	Unauthorised system access	40,178 individuals. Names, Social Security numbers, driving licence numbers and passport numbers	Sector Technology

1.2 Incident Analysis

Identity-Based Intrusion

The Carnival Corporation breach is the most instructive identity incident of the quarter. A threat actor working under the ShinyHunters banner talked an employee into granting access to a portion of the corporate IT estate, and from there reached data tied to the Holland America Mariner Society loyalty programme. The company confirmed approximately 8.7 million records with 7.5 million unique email addresses, covering names, dates of birth, gender, passport numbers and loyalty status. More than 800,000 residents of Texas alone received notification. Detection came on 14 April, and the breach notice followed on 27 May, a gap of six weeks between discovery and public disclosure.

Aman Resorts and 7-Eleven appeared on the same pay-or-leak warning list on 18 April, both attributed to compromise of their Salesforce environments. The Aman listing claimed more than 500,000 records holding personal data, with a ransom deadline of 21 April. Neither claim has been independently verified. The pattern across all three victims is consistent. The attacker did not defeat a firewall or exploit a software flaw in the customer relationship platform itself, and instead obtained legitimate credentials or a legitimate session through human manipulation. Organisations that treat their Salesforce tenancy as a trusted internal system, when it is an internet-facing repository of guest and customer data, are carrying more exposure than their architecture diagrams suggest.

BWH Hotels illustrates a different failure. A flaw in a web application holding guest reservation data gave an intruder access from 14 October 2025 until identification on 22 April 2026, a period of just over six months. Guest names, contact details, home addresses, reservation numbers, dates of stay and special requests were reachable throughout. Payment and banking data was held elsewhere and was not affected, which limited the financial consequence without limiting the privacy consequence.

Ransomware and Exfiltration

Qilin dominated sector ransomware activity during Q2 2026. The group listed Sysco in early May with a negotiation deadline of 12 May, added an Australian hospitality and gaming technology supplier on 15 May, and then produced a claim spree between 2 and 5 June that swept up Jay’s Catering, Don Don Group and InterSPA-Gruppe. Eat Salad followed on 3 June, Avcon Jet on 4 June with sample files published, and Sivatel Bangkok on 21 June. NordStellar recorded 299 Qilin leak site listings across the quarter, with The Gentlemen close behind on 284 and overtaking Qilin during June.

DragonForce claimed approximately 352 GB from Gelatissimo in Australia and published sample files covering employee records, financial information and internal documents. The company acknowledged an investigation. AUDIT TEAM listed Mopaş Online Supermarket in Turkey, and the company confirmed the breach after the listing appeared, one of the few claims in this quarter to receive victim confirmation. The Hotelogix and Treebo case attributed to shadowbyt3$ rests on misconfigured cloud storage and involved no intrusion in the conventional sense, with guest folios, stay details, room numbers and partial payment card data reachable through bulk scraping and a demand of 500,000 US dollars attached.

Food service absorbed the sharpest increase in this activity. Comparitech logged 640 ransomware attacks globally during April and 661 during May, with food and beverage companies recording the steepest sectoral rise at 80% month on month. Ransomware accounted for 48% of all data breaches tracked globally in the Verizon 2026 Data Breach Investigations Report.

The Authentication Laundering Campaign

This campaign began during April 2026 and continues. Microsoft disclosed it on 25 June and named the technique authentication laundering, because the phishing messages are routed through Calendly notification infrastructure and therefore arrive from a legitimate, authenticated sending service. Messages of this kind pass SPF and DKIM checks and clear standard email security filters without difficulty, since the sending domain is genuine and holds a clean reputation.

The payload is a Node.js implant that runs in memory and leaves no file on disk, which defeats signature-based endpoint tools that scan the file system. Compromised machines beacon to command and control infrastructure over non-standard ports. Microsoft identified the affected devices through their names, which include reception, frontdesk, reservations, accueil and recepce, and those machines hold sessions into property management systems, payment infrastructure, guest databases and reservation platforms. Hotels across Europe and Asia are affected and no group has claimed the campaign. Any property whose front-office staff receive external booking and meeting notifications should treat this as a current threat.

Contested Claims and Narrative Pressure

Eleven of the twenty in-scope incidents this quarter rest on a threat actor claim alone, with no independent verification and no victim statement. Qilin holds a documented record of leak site posts that are never substantiated with published data, so the June claim spree should be read as an assertion of capability as much as a record of successful attacks. The Ryanair case follows a comparable pattern. An actor offered material on a hacker forum in late April, described as data from a legal claims management platform covering EU Regulation 261/2004 compensation cases, internal legal correspondence, flight data and banking details. No confirmation has followed.

Booking.com deserves separate mention. The company notified customers on 12 and 13 April of unauthorised third-party access to reservation records, and the stolen material moved into payment-redirection phishing against travellers almost at once. No group has claimed the incident and the company has not named a vector. The surface similarity to the PHALT#BLYX campaign covered in the Q1 edition is real but unproven, and linking the two without evidence would be a mistake.

Supply Chain and Third-Party Risk

Alsea, the Latin American operator of Domino’s, Starbucks and Vips outlets, suffered no direct breach of its own systems. A third-party technology vendor was compromised and exposed 12.6 GB of material including plaintext credentials, transaction records, security audit reports and live surveillance camera access, with Alsea named among the affected clients. The Australian hospitality and gaming technology supplier listed by Qilin on 15 May carries the same shape of risk for every downstream operator dependent on its platform.

More than 100 hotels in the Netherlands, with further reports from Belgium and Ireland, lost customer and reservation data during early June through what investigators believe to be a vulnerability in shared booking software. Criminals reused that data at once in phishing messages demanding payment under threat of cancellation. One flaw in one widely deployed application produced simultaneous exposure across three countries and more than a hundred independent businesses, none of which had any control over the software concerned.

1.3 Key Findings for Q2 2026

- Twenty incidents documented across hotel, restaurant and food service, tourism and travel, and sector technology sub-sectors during Q2 2026, with two further Q1 attacks reaching disclosure inside the quarter.
- Identity compromise through social engineering of cloud customer relationship platforms produced the largest breaches of the quarter and defeated technical controls without touching them.
- Eleven of twenty incidents rest on unverified threat actor claims, and leak site listing dates should never be read as intrusion dates.
- The authentication laundering phishing campaign against hotel front-office workstations is active and ongoing, and any property whose reception staff receive external notification email is in scope.
- Check Point Research recorded an average of 2,291 weekly cyberattacks per organisation across hospitality, travel and recreation during May 2026, a rise of 24% year-on-year against a global all-industry rise of 2%, and a cumulative rise of 122% since May 2023.
- Dwell time remains the quiet problem, with the BWH Hotels intrusion running undetected for six months and the Carnival disclosure arriving six weeks after detection.
- Third-party technology providers, covering Alsea's vendor, the Australian gaming supplier, Hotelogix and the shared European booking platform, account for the widest blast radius of any single failure this quarter.
- Guest-held data including passport details, loyalty records and stay histories carries regulatory and reputational exposure out of proportion to its volume, and stolen reservation data now moves into payment-redirection fraud within days and no longer within months.
- SecureTrust research published during May 2026 found that 92% of travel agencies experienced a cyber threat in the preceding twelve months and 66% reported customer data compromises, placing cyber risk ahead of inflation and recession as the leading threat to agency success.

2. Incident Overview

Between April and June 2026, twenty organisations across the hotel, restaurant, food service and tourism sectors were hit by cyberattacks. Two attacks from the first quarter also became public during this period. One sustained social engineering campaign targeted hotel front-office staff across Europe and Asia. This section explains how those attacks happened, what the attackers wanted, and what the damage looked like. The full incident matrix, mapping each attack against five stages of a typical intrusion, is in Appendix A. The sector summary in 2.2 gives a quick breakdown by industry.

2.1. How the Attacks Unfolded

Initial Access (how attackers got in)

The most common entry method this quarter was the manipulation of a person, and not the exploitation of a IT system. At Carnival Corporation, an attacker working for ShinyHunters persuaded an employee to grant access to a portion of the corporate IT estate, and from this single conversation reached data covering 8.7 million records. Aman Resorts and 7-Eleven were compromised through their Salesforce environments in the same fortnight and appeared on a pay-or-leak warning list on 18 April. In each case the customer relationship platform performed exactly as designed, and the attacker arrived holding what the system understood to be a legitimate identity.

Software flaws still opened doors. BWH Hotels traced its breach to a weakness in a web application holding guest reservation data, and this weakness gave an intruder access from 14 October 2025 until identification on 22 April 2026. Hotelogix and Treebo lost guest folios through misconfigured Amazon S3 buckets and Azure blob storage that permitted bulk scraping without any intrusion at all. More than 100 hotels across the Netherlands, Belgium and Ireland lost reservation data during early June through what investigators believe to be a vulnerability in shared booking software none of them controlled.

For hotel and restaurant organisations, this means the perimeter is now a person, a cloud tenancy and a supplier release cycle. A firewall rule protects none of the three.

Execution and Persistence (what the attackers ran and how they stayed)

Ransomware deployment dominated the volume figures. Qilin listed Sysco in early May with a negotiation deadline of 12 May, added an Australian hospitality and gaming technology supplier on 15 May, and produced a claim spree between 2 and 5 June that swept up Jay’s Catering, Don Don Group and InterSPA-Gruppe, followed by Eat Salad, Avcon Jet and Sivatel Bangkok. DragonForce encrypted and exfiltrated at Gelatissimo, publishing sample files to prove the claim. AUDIT TEAM listed Mopaş Online Supermarket, and the company confirmed the breach after the listing appeared.

The phishing campaign against hotel front offices took a quieter path. Messages arrived through Calendly notification infrastructure and delivered a Node.js implant that runs entirely in memory and writes nothing to disk. Persistence came from the session itself and from repeated delivery to the same reception mailboxes, which removed the need for a startup entry or a registry key that an endpoint tool might notice. Compromised machines beaconed to command-and-control infrastructure over non-standard ports.

For hotel IT teams, the message has shifted since the last edition. Ransomware remains the loudest threat, and a payload that leaves no file behind defeats the file-scanning controls most properties still depend on.

Credential Access and Evasion (how attackers stole logins or avoided detection)

Several attacks succeeded because the attacker looked like a legitimate user or arrived from a legitimate service. Microsoft named the technique behind the hotel campaign authentication laundering on 25 June, because the phishing messages are routed through a genuine, authenticated sending platform. Messages of this kind pass SPF and DKIM checks and clear standard email security filters without difficulty, since the

sending domain is real and carries a clean reputation. No filter rule based on sender reputation will stop them.

The Salesforce intrusions attributed to ShinyHunters rest on the same principle applied to identity. An attacker who holds a valid session or a legitimate set of credentials produces monitoring output that looks like ordinary business activity. The Booking.com breach shows the downstream version of the problem, where guest names, contact details, booking dates and free-text notes to hotels were reused within days in payment-redirection phishing that appeared credible to travellers precisely because it quoted their real reservation.

For organisations that rely on multi-factor authentication as their primary defence, these incidents show that authentication controls settle the question of who logged in and answer nothing about what that identity then did. Session monitoring, token revocation and anomaly detection on data access remain the missing controls.

Collection and Exfiltration (what attackers took and how they moved it out)

The volume of stolen data across the quarter was substantial. ShinyHunters took approximately 8.7 million records from Carnival Corporation, holding 7.5 million unique email addresses. DragonForce claimed 352 GB from Gelatissimo. The Alsea vendor exposure ran to 12.6 GB. ShinyHunters claimed more than 500,000 records from Aman Resorts, and shadowbyt3$ attached a demand of 500,000 US dollars to the Hotelogix and Treebo folios.

The type of data varied by sub-sector. Hotels lost guest names, contact details, home addresses, dates of stay and special requests through BWH Hotels, and guest folios with room numbers and partial payment card data through Hotelogix. Restaurants and food service operators lost employee records, financial information and internal documents through Gelatissimo, and plaintext credentials, transaction records and live surveillance camera access through the Alsea vendor. Tourism organisations lost passport numbers, dates of birth and loyalty status through Carnival, and reservation records through Booking.com.

For any organisation that holds guest personal data, payment references or employee records, these incidents confirm that stolen reservation data now converts into fraud within days. The question is not whether attackers will try to steal data. It is how quickly the organisation can detect the loss and warn the guests whose details are already in circulation.

Impact (what it cost the organisations)

The damage this quarter fell more heavily on privacy and trust than on operations. More than 800,000 residents of Texas alone received notification following the Carnival breach, and the company disclosed on 27 May having detected the intrusion on 14 April. BWH Hotels disclosed on 11 May an intrusion that had run for six months. Travellers holding Booking.com reservations received convincing payment-redirection messages within days of the theft, and hotel guests across the Netherlands, Belgium and Ireland received demands for payment under threat of cancellation.

Regulatory exposure across the quarter is heavy. Passport numbers and dates of birth taken from Carnival, passport and driving licence numbers taken from RCI Internet Services, and Social Security numbers taken from Taos Mountain Casino all sit in the most heavily protected categories under European and United States law. Operational disruption, by contrast, was barely reported, and no incident this quarter produced a confirmed shutdown of payment terminals or building systems.

For risk managers, the absence of operational disruption should not read as an improvement. Attackers took the data and left the systems running, which removes the visible signal that historically triggered incident response and lengthens the window before anyone notices.

2.2 Sector Summary

Attribution and threat landscape

Across the quarter, attribution remained a problem. Eleven of the twenty incidents rely on a threat actor claim alone, with no independent verification and no victim statement. Only Carnival, BWH Hotels, Booking.com and Mopaş provided reliable dates or confirmations.

NordStellar recorded 299 Qilin leak site listings during the quarter against 284 for The Gentlemen, which rose 39% on Q1. Breachsense recorded The Gentlemen overtaking Qilin during June with 94 claimed victims. Comparitech logged 640 ransomware attacks globally in April and 661 in May, bringing the first half total to 4,217, an increase of 11% on the second half of 2025.

For a risk manager, this means that the number of listings on leak sites says more about how active the criminal market is than about how many organisations were actually hit. Behavioural monitoring and keeping systems separate remain the more reliable defences.

Sector	Incidents	Identity or Token Abuse	Ransomware	Supply Chain	Payment Affected	OT Disruption	Social Engineering
Hotel	4 + 1 campaign	1	1	1	0	0	2
Restaurant and Food Service	8	1	6	1	0	0	0
Tourism and Leisure	5	1	2	0	1	0	2
Infrastructure	2	0	1	2	1	0	0

Note: Individual incidents may appear in more than one column where multiple categories apply. For example, the Hotelogix and Treebo exposure involved a technology supplier, reached partial payment card data and originated in cloud misconfiguration. Column totals will therefore exceed the incident count for that row.

Patterns by sub-sector

Ransomware accounted for ten of the twenty incidents and hit restaurant and food service operators hardest. They absorbed six of those claims across a single month.

Identity and token abuse appeared in three incidents across the hotel, restaurant and tourism sub-sectors. Each of those three produced the largest data volumes of the quarter. This shows that a small number of identity failures carry a disproportionate share of the total exposure.

Supply chain and third-party risk appeared in four incidents. These covered Alsea's vendor, the Australian gaming supplier, Hotelogix and the shared European booking platform. That last case alone reached more than a hundred independent hotels across three countries.

Payment data was affected at two organisations. Operational technology disruption was recorded nowhere. This is a marked change from Q1 2026, when payment terminals and ticketing systems were taken offline at four organisations.

One sustained social engineering campaign targeted hotel front-office staff across Europe and Asia. A second wave of phishing reused stolen reservation data against guests. Both exploited the reservation workflow, not any technical weakness in the properties themselves.

3. Threat Actor Profiles

3.1 The Threat Actor Landscape

Five named threat actors are confirmed to have carried out attacks against hotels, restaurants, food service and tourism organisations during this period. A sixth group is included because of its activity across other sectors. This is a smaller named set than the eleven actors recorded in Q1 2026. The reduction reflects the state of public reporting, not a fall in criminal activity.

Six of the twenty incidents this quarter have no known attacker. This includes the Booking.com breach, the BWH Hotels intrusion and the sustained phishing campaign against hotel front offices. Two actors account for eleven of the fourteen incidents that have been attributed. The table below summarises each group and its assessed risk level to this sector.

Threat Actor	Also Known As / Affiliations	Preferred Tactics	Q2 2026 Sector Targets	Data Scale	Risk to Sector
ShinyHunters / Scattered Lapsus$ Hunters	ShinySp1d3r RaaS; The Com; Trinity of Chaos	Social engineering of employees; Salesforce environment compromise; pay-or-leak extortion with dated deadlines	Carnival Corporation (8.7 million records); Aman Resorts (500,000 records claimed); 7-Eleven (categories undisclosed)	Up to 8.7 million records per target	Critical
Qilin	Agenda (original name)	RaaS; double extortion; high-volume leak site listing; proof-of-claim releases; short negotiation deadlines	Sysco; Australian hospitality and gaming IT supplier; Eat Salad; Jay's Catering; Don Don Group; InterSPA-Gruppe; Avcon Jet; Sivatel Bangkok	299 leak site listings across all sectors; sector data volumes unconfirmed	Critical
DragonForce	DragonForce Malaysia; operates a cartel affiliate model	Ransomware with exfiltration; sample file publication to substantiate claims; large-volume theft	Gelatissimo (352 GB claimed); Taos Mountain Casino (38.6 GB, March attack disclosed in Q2)	Up to 352 GB per target	High
The Gentlemen	TheGentlemen; Gentlemen Ransomware	RaaS; multi-OS encryption; SystemBC proxy botnet; EDR evasion; rapid affiliate growth	No named hotel, restaurant or tourism victim confirmed in Q2 2026	284 leak site listings across all sectors, a rise of 39% on Q1	High
AUDIT TEAM	No confirmed aliases or rebrand	Ransomware; leak site extortion; targeting of food retail and regional operators	Mopaş Online Supermarket, Turkey (breach confirmed by the victim)	Data volume unconfirmed	Moderate
shadowbyt3$	No confirmed aliases or rebrand	Cloud storage misconfiguration discovery; bulk scraping without intrusion; direct ransom demand	Hotelogix and Treebo Hotels, Singapore and India (guest folios and partial card data)	USD 500,000 demand; record count unconfirmed	Moderate

3.2 Adversary Behaviour Patterns

Three patterns define the adversary set in this quarter and have direct implications for how organisations should defend themselves.

Identity Attacks Have Moved to the Customer Relationship Platform

ShinyHunters remains the highest-risk actor for this sector, and its method has narrowed rather than broadened. The group did not exploit a software flaw at Carnival Corporation, Aman Resorts or 7-Eleven. It gained access to Salesforce environments. In the Carnival case, this happened through a conversation with an employee who granted access. The customer relationship platform now holds the guest and loyalty data

that once sat behind a corporate firewall. It authenticates anyone who presents a valid identity, without questioning why that identity has started reading eight million records. Carnival detected the intrusion on 14 April and disclosed it on 27 May, a gap of six weeks. BWH Hotels carried an intruder for six months. An organisation can be actively losing data while its security indicators show nothing unusual.. An organisation can be under active exfiltration while its security indicators show nothing unusual.

Supply Chain and Vendor Exposure

The second pattern is the widening supply chain attack surface. This quarter it produced the single largest blast radius of any failure. More than 100 hotels across the Netherlands, Belgium and Ireland lost reservation data through a probable flaw in shared booking software that none of them controlled or could patch. Qilin's attack on an Australian hospitality and gaming technology supplier is an attack on every operator running that platform. The Alsea case shows a third variant. A technology vendor exposed 12.6 GB including plaintext credentials, transaction records and live surveillance camera access, naming Alsea among the affected clients. Hotelogix and Treebo lost guest folios through misconfigured cloud storage, which required no intrusion at all. Organisations cannot assess their own exposure without understanding the security posture of the vendors, platforms and cloud tenancies they depend on.

Volume Competition and Claim Inflation

The third pattern is a contest for market position among ransomware operators, conducted through leak site volume. NordStellar recorded 299 Qilin listings across the quarter against 284 for The Gentlemen, which rose 39% on Q1. Breachsense recorded The Gentlemen overtaking Qilin during June with 94 claimed victims. Qilin's sector activity fits that contest more closely than any operational logic. It posted three claims between 2 and 5 June and listed eight sector victims across the quarter, most of them small operators with no disclosed data volumes. Eleven of the twenty incidents rest on a claim alone. A listing establishes reputation among affiliates whether or not the underlying attack succeeded. So the volume figures measure the confidence of the criminal market and overstate the number of organisations actually compromised.

What this means for organisations in these sectors

The adversary set is narrower than last quarter and its methods are more uniform. This makes the defensive priority easier to state, but no easier to deliver. Controls that work regardless of which group is attacking remain identity governance and session monitoring inside cloud platforms, contractual and technical assurance over vendors and shared booking software, audit of cloud storage permissions, and incident response plans tested against realistic scenarios drawn from the incidents in this report. For most hotels, restaurants and tourism businesses, the weakest point is not the network boundary or the devices staff use but the platforms that store guest data for the organisation and control who can access it.

4. Cyber Threat Trends

Top six cyber threat trends observed from April to June 2026

Trend 1. Phishing now arrives from services you already trust

Email security has been built for a decade around the question of whether the sender is genuine. Attackers have answered this question by making the sender genuine. The campaign against hotel front offices that ran from April and was disclosed by Microsoft on 25 June routed its phishing messages through the Calendly notification infrastructure, a legitimate scheduling service with a clean sending reputation. Microsoft named the technique authentication laundering. Messages sent this way pass SPF and DKIM checks, clear standard filters and carry no reputational signal that would mark them as suspicious, because every technical indicator confirms exactly what it is asked to confirm. Check Point Research identified three coordinated bulk-registration phishing campaigns in the same period, including more than 210 sequentially numbered hotel-lure domains, a Chinese-language Booking.com impersonation cluster and a Canada-focused Airbnb impersonation domain. Filter rules based on sender reputation will not stop a message that arrives from a service the organisation already permits.

Who is affected: Hotels and tourism organisations most of all, and any organisation whose staff get external booking or meeting notifications as part of their normal work.

Trend 2. Attackers are talking their way into your customer relationship platform

The biggest breaches this quarter started with a conversation. At Carnival Corporation, an attacker working for ShinyHunters persuaded an employee to grant access to part of the IT system. They got about 8.7 million records from the Holland America loyalty programme. Aman Resorts and 7-Eleven appeared on the same pay-or-leak warning list on 18 April, both through their Salesforce systems. Guest data, loyalty histories and marketing records now sit in cloud platforms that are outside the corporate network. These platforms check who is logging in, but they do not check what that person does once they are in. In each case, the platform worked exactly as designed. It confirmed who was logging in and asked nothing about what that identity then read. Organisations that treat Salesforce as a trusted internal system, when it is actually an internet-facing store of guest data, have more exposure than their architecture diagrams show.

Who is affected: Hotels, restaurants, food service, tourism, and any organisation that holds customer or loyalty data in a cloud platform.

Trend 3. Stolen reservation data is used within days

The time between a breach and criminals using the data against guests has become very short. Booking.com told customers on 12 and 13 April that someone had accessed reservation records. The stolen data included names, contact details, home addresses, booking dates and notes to hotels. Criminals started sending fake payment requests to those travellers almost immediately. The messages worked because they quoted real bookings. The same thing happened in early June across more than 100 hotels in the Netherlands, with more reports from Belgium and Ireland. Stolen data was used to demand payment under threat of cancellation. A guest who gets a message with their real booking reference, arrival date and room type has little reason to doubt it. The organisation that lost the data may still be investigating while its guests are already losing money.

Who is affected: Hotels, tourism, and any operator that holds future reservations with guest contact details.

Trend 4. Malware that never touches the disk

Most endpoint protection still works by scanning files. The malware used in the hotel phishing campaign is written in Node.js and runs entirely in memory. It writes nothing to disk, so there is nothing for a scanner to find. Compromised machines send signals to command-and-control systems over non-standard ports. Microsoft identified them through their device names (in this quarter reception, frontdesk, reservations,

accueil and recepce). These machines have live connections to property management systems, payment systems, guest databases and reservation platforms. They are the most valuable endpoints in the building and the least likely to be rebuilt or patched during a busy season. Malware that leaves no trace defeats signature-based tools by design and detection has to look at what the machine does, not what it stores.

Who is affected: All sectors. Hotels and tourism are at higher risk because of the number of shared, always-on front-desk terminals in daily use.

Trend 5. Misconfigured cloud storage is now a breach type on its own

Hotelogix and Treebo Hotels lost guest folios, contact details, arrival and departure dates, room numbers and partial payment card data to an attacker called shadowbyt3$. No one broke into the system. The cloud storage had been set up to allow bulk scraping, so the data was simply collected by asking for it. A ransom demand of 500,000 US dollars followed. Nothing in this incident would show up in an intrusion detection log, because there was no intrusion in the normal sense. Cloud storage permissions are set once during a deployment, rarely reviewed and almost never covered by penetration tests. For property management vendors that hold data for hundreds of hotels, one permission error exposes all of them at once.

Who is affected: All sectors, and property management, booking and loyalty platform vendors in particular.

Trend 6. Leak site volume reflect cybercriminal competition, not your risk

Ransomware groups spent this quarter competing for position. NordStellar recorded 299 Qilin leak site listings against 284 for The Gentlemen, which rose 39% on Q1. Breachsense recorded The Gentlemen overtaking Qilin during June with 94 claimed victims. Qilin posted three sector claims between 2 and 5 June alone. Eleven of the twenty incidents in this report are based on a claim with no independent verification and no victim statement. Qilin has a record of listings that are never backed up with published data. A listing builds reputation among affiliates whether or not the attack succeeded, so every group has a reason to claim more than it actually has. Comparitech logged 640 ransomware attacks globally in April and 661 in May. The first half total was 4,217, up 11% on the second half of 2025. Food and beverage companies had the sharpest rise at 80% month on month. These figures show a market that is growing but do not tell a risk manager how many organisations were actually hit.

Who is affected: All sectors. Restaurants and food service operators saw the sharpest increase in claims this quarter.

5. Tactics, Techniques and Procedures

This section looks at the specific methods attackers used against hotels, restaurants, food service and tourism organisations in Q2 2026. Each part describes a confirmed technique, explains how it worked, and sets out what it means for your organisation.

5.1 Social Engineering: The Authentication Laundering Campaign

The most persistent attack of Q2 2026 did not start with malware. It started with a meeting notification. From April onwards, hotel front-office staff across Europe and Asia received phishing messages sent through Calendly notification infrastructure. Calendly is a legitimate scheduling service used across the business world. Microsoft disclosed the campaign on 25 June and named the technique authentication laundering, because the message inherits the authentication and reputation of the service that sends it.

Messages sent this way pass SPF and DKIM checks and get through standard email filters, because the sending domain is genuine and has a clean history. Staff see a notification from a service their organisation already allows, arriving in the middle of a working day spent processing exactly this kind of external request. The technique exploits the routine of the reception desk, not a technical weakness in the systems. No filter rule based on sender reputation will separate the malicious message from the thousands of legitimate ones that arrive alongside it.

5.2 Memory-Resident Payloads and Fileless Persistence

The hotel campaign also used a second technique that security teams need to understand. The payload is written in Node.js and runs entirely in memory. Nothing is written to the file system, so there is no file for an antivirus scanner to find, quarantine or match against a signature. Persistence comes from the live session and from repeated delivery to the same reception mailboxes. This removes the need for a startup folder shortcut or a registry entry that endpoint tools are set up to watch.

Compromised machines send signals to command and control systems over non-standard ports. Microsoft identified the affected devices through their names, such as reception, frontdesk, reservations, accueil and recepce. These machines have live connections to property management systems, payment infrastructure, guest databases and reservation platforms. The practical result is that endpoint security built around file scanning will not detect this attack. Detection has to rely on network behaviour, especially outbound connections on unexpected ports from workstations whose normal traffic is well understood.

5.3 Salesforce Environment Compromise and Pay-or-Leak Extortion

ShinyHunters compromised Carnival Corporation, Aman Resorts and 7-Eleven during April 2026 through their Salesforce environments. Salesforce is a cloud platform that holds customer records, loyalty histories and marketing contact data. It sits outside the corporate network by design so that staff can reach it from anywhere. Access depends on identity, not on network location.

At Carnival, the attacker obtained that identity by persuading an employee to grant access to part of the IT system. From there they reached about 8.7 million records containing names, dates of birth, gender, passport numbers and loyalty status. Aman Resorts and 7-Eleven appeared together on a pay-or-leak warning list on 18 April. The Aman listing claimed more than 500,000 records and carried a ransom deadline of 21 April. The extortion model attaches a deadline to a claim of data already held. This shifts the pressure from system recovery to disclosure timing and gives the victim no technical remedy at all.

5.4 Helpdesk and Employee Social Engineering

The Carnival breach turned on a single conversation. An attacker approached an employee, established enough credibility to be treated as a legitimate request, and was granted access. No credential was cracked

and no vulnerability was exploited. The access that followed looked completely normal to monitoring systems, because it was normal in every technical sense.

Hotel, restaurant and tourism organisations are structurally exposed to this method. High staff turnover, seasonal recruitment, distributed properties and a service culture that trains people to be helpful all work in the attacker's favour. Verification procedures for access requests need to be specific enough that a staff member can say no to a plausible request without feeling obstructive. The procedure also has to survive a busy shift, a new starter and a caller who sounds senior.

5.5 Third-Party Vendor Compromise and Credential Exposure

Alsea, the Latin American operator of Domino's, Starbucks and Vips outlets, did not suffer a breach of its own systems. A third-party technology vendor was compromised and exposed 12.6 GB of material. This included plaintext credentials, transaction records, security audit reports and live surveillance camera access. Alsea was named among the affected clients. Credentials stored without encryption in a vendor environment give an attacker a working key to every system those credentials open, including systems the vendor does not operate.

Qilin's attack on an Australian hospitality and gaming technology supplier on 15 May carries the same kind of risk for every operator running that platform. The attack surface for hotel and restaurant organisations now reaches well beyond their own IT perimeter. Contractual assurance that a vendor holds a certification is not the same as knowing how that vendor stores the credentials it holds on your behalf.

5.6 Cloud Storage Misconfiguration and Bulk Scraping

Hotelogix and Treebo Hotels lost guest data during April and May 2026 to an attacker operating as shadowbyt3$. No intrusion took place. Amazon S3 buckets and Azure blob storage had been configured to allow access without authentication, so the data was collected by simply requesting it. Guest folios, names, telephone numbers, home addresses, arrival and departure dates, room numbers and types were taken, along with payment fields covering the last four digits of cards, transaction identifiers and billing amounts. A ransom demand of 500,000 US dollars followed.

An incident like this generates no intrusion alert, because nothing was breached. Storage permissions are set during deployment, rarely reviewed afterwards and often left out of penetration testing scopes written for network infrastructure. For a property management vendor holding data for hundreds of hotels, one permission error exposes all of them at once. The hotels concerned have no visibility of the setting and no ability to fix it.

5.7 Web Application Flaws and Extended Dwell Time

BWH Hotels disclosed on 11 May that a flaw in a web application holding guest reservation data had given an intruder access from 14 October 2025 until 22 April 2026. Guest names, email addresses, telephone numbers, home addresses, reservation numbers, dates of stay and special requests were accessible throughout that period. Payment and banking data was held in a separate system and was not affected. This limited the financial consequence but not the privacy consequence.

Six months of undetected access is the real finding here, not the flaw itself. Carnival detected its intrusion on 14 April and disclosed on 27 May, a gap of six weeks. Guest-facing web applications are built for availability and revenue, deployed under commercial deadlines, and monitored for uptime, not for unusual data access. Where logging of read activity does not exist, the length of an intrusion is worked out after the fact by inference. Every day of that period represents guests who were never warned.

5.8 Third-Party Booking Platform Risk (Shared Reservation Software)

More than 100 hotels in the Netherlands, with further reports from Belgium and Ireland, lost customer and reservation data in early June 2026 through what investigators believe to be a vulnerability in shared hotel booking software. Independent properties across three countries were exposed at the same time by one flaw in one application. None of them could patch it, audit it or know that it existed.

Booking platforms and channel managers connect directly into hotel property management systems to synchronise availability, pricing and reservation data in real time. The integration is a legitimate and necessary business tool. But it concentrates risk in a way that individual properties cannot manage through their own controls. Reservation data is also the most immediately monetisable data a hotel holds. It identifies a named guest, a future date and an expected payment, which is everything a payment-redirection fraud needs.

5.9 Downstream Guest-Directed Fraud

Stolen reservation data was used against guests within days on two separate occasions this quarter. Booking.com notified customers on 12 and 13 April, and criminals were already sending payment-redirection messages to those travellers. The June breach across the Netherlands, Belgium and Ireland produced messages demanding payment under threat of cancellation. In both cases the fraud worked because the message quoted a genuine booking. This removed the inconsistency that normally allows a recipient to spot a scam.

The organisation that lost the data carries the reputational damage even when the fraud is carried out by a third party against a guest using a channel the organisation does not control. For hotel and tourism operators, the practical point is about communications as much as security. Guests need to know, before an attacker contacts them, how the property will and will not ask for payment. That message has to be given at the point of booking, not in a breach notification sent weeks after the data has already been traded.

6. Sector Specific Risk Profiles

This section explains the structural conditions that make each sector a target. It also covers what data is at risk and which attack methods were confirmed by Q2 2026 incidents. General managers and risk managers can use this section to understand why attackers find their environment attractive and where their biggest exposures are.

6.1 Hotels

Hotels remain among the most attractive targets in the private sector. The Q2 2026 evidence shows the point of attack moving away from the property itself and towards the platforms that serve it. Guest names, passport numbers, home addresses, arrival dates and special requests now sit in reservation systems, property management platforms and cloud storage operated by vendors. A hotel has no visibility of how those systems are configured.

Check Point Research recorded an average of 2,291 weekly cyberattacks per organisation across hospitality, travel and recreation during May 2026. This is a rise of 24% year on year against a global all-industry rise of 2%, and a cumulative rise of 122% since May 2023.

BWH Hotels shows what happens when a guest-facing web application has a flaw. An intruder held access to reservation data from 14 October 2025 until 22 April 2026, a period of just over six months. The affected system did not hold payment or banking data, so the financial consequence was limited but the privacy consequence was not.

More than 100 hotels across the Netherlands, with further reports from Belgium and Ireland, lost reservation data in early June through a probable vulnerability in shared booking software. None of those properties controlled or could patch the software. Hotelogix and Treebo Hotels lost guest folios through misconfigured cloud storage. This exposure required no intrusion at all.

The front desk itself became a defined target this quarter. The phishing campaign disclosed by Microsoft on 25 June identified compromised machines through device names including reception, frontdesk, reservations, accueil and recepce. Those workstations hold live sessions into property management systems, payment infrastructure, guest databases and reservation platforms.

Aman Resorts was listed by ShinyHunters on 18 April with a claim of more than 500,000 Salesforce records and a deadline of 21 April. Sivatel Bangkok was listed by Qilin on 21 June.

Confirmed attack vectors across these cases include phishing through legitimate notification services, memory-resident implants on front-office terminals, cloud storage misconfiguration, web application flaws with long-term access, and compromise of shared booking software.

Data Assets at Risk

Data Asset	Detail and Q2 2026 Evidence
Guest PII	Full names, passport numbers, home addresses, email addresses, telephone numbers, dates of birth. BWH Hotels. Guest names, contact details, home addresses, reservation numbers, dates of stay and special requests reachable for six months.
Reservation data	Booking references, arrival and departure dates, room numbers and types, free-text notes to the property. Booking.com and the multi-country European breach both produced reservation data that criminals reused in guest-directed fraud within days.

Data Asset	Detail and Q2 2026 Evidence
Guest folio and payment fields	Last four digits of cards, transaction identifiers, billing amounts. Hotelogix and Treebo. Folio data reachable through misconfigured cloud storage with a demand of 500,000 US dollars attached.
Front-office session access	Live authenticated sessions into property management, payment and reservation systems held on shared reception terminals. Identified by Microsoft as the target of the authentication laundering campaign running from April 2026.
Loyalty and cloud platform records	Membership data, contact histories and marketing records held in customer relationship platforms outside the corporate network. Aman Resorts. More than 500,000 Salesforce records claimed by ShinyHunters.

RISK: HIGH Hotels hold the broadest and most valuable data profile of any sector covered by this report, and the Q2 2026 evidence shows that the material exposures now sit outside the property. Shared booking software, vendor-operated cloud storage and cloud customer relationship platforms produced three of the four hotel incidents this quarter, and the front-desk workstation has become a named target in its own right.

6.2 Restaurants and Food Service

Restaurant and food service operators saw the sharpest rise in claimed attacks this quarter. Comparitech logged 640 ransomware attacks globally in April 2026 and 661 in May. Food and beverage companies had the steepest sectoral rise at 80% month on month. Eight of the twenty incidents in this report fall in this sub-sector.

Thin IT resources, high staff turnover, distributed sites and heavy reliance on external platforms for ordering, delivery, payment and marketing create a wide third-party attack surface that individual operators cannot monitor.

Qilin dominated the claims. Sysco was listed in early May with a negotiation deadline of 12 May and screenshots of alleged internal documents. Jay's Catering, Don Don Group and Eat Salad followed during the June claim spree. DragonForce claimed about 352 GB from Gelatissimo and published sample files covering employee records, financial information and internal documents. AUDIT TEAM listed Mopaş Online Supermarket in Turkey, and the company confirmed the breach. This made it one of the few claims this quarter to receive victim confirmation.

Alsea, the Latin American operator of Domino's, Starbucks and Vips outlets, shows the vendor problem in its clearest form. No breach of Alsea systems occurred. A third-party technology vendor was compromised and exposed 12.6 GB of material. This included plaintext credentials, transaction records, security audit reports and live surveillance camera access. Alsea was named among the affected clients.

7-Eleven appeared on the ShinyHunters pay-or-leak warning list on 18 April through its Salesforce environment.

Confirmed attack vectors for the sector include ransomware with data theft against operators of all sizes, third-party vendor credential exposure, and social engineering of cloud platform access.

Data Assets at Risk

Data Asset	Detail and Q2 2026 Evidence
Employee and HR records	Names, contact details, payroll and financial information, internal documents. Gelatissimo. Sample files published by DragonForce from approximately 352 GB claimed.

Data Asset	Detail and Q2 2026 Evidence
Vendor-held credentials	Plaintext passwords, transaction records, security audit reports and live surveillance camera access. Alsea. 12.6 GB exposed through a third-party technology vendor with no breach of Alsea systems.
Customer and cloud platform data	Contact records, marketing histories and loyalty data held in customer relationship platforms. 7-Eleven. Named on the ShinyHunters pay-or-leak warning list of 18 April through a Salesforce environment.
Corporate and operational data	Internal documents, supplier agreements, distribution records. Sysco. Leak site listing carrying screenshots of alleged internal documents with a negotiation deadline of 12 May.
Confirmed system compromise	Mopaş Online Supermarket. Breach of systems confirmed by the company following the AUDIT TEAM listing, one of the few Q2 claims corroborated by the victim.
RISK: HIGH Ransomware claims against this sub-sector rose faster than any other during Q2 2026, and eight of the twenty in-scope incidents fall here. Most of those claims rest on a leak site listing alone, which means the true rate of compromise is unknown and probably lower than the volume suggests. The Alsea case shows that an operator can lose credentials, transaction records and camera access without any attacker touching its own systems.	

6.3 Tourism and Travel

Tourism operators hold itinerary data for large numbers of customers. The value of that data to an attacker is about context, not volume. A traveller who gets a message quoting their real booking reference, arrival date and property has little reason to doubt it.

Q2 2026 confirmed that the time between theft and exploitation has become very short. Booking.com told customers on 12 and 13 April about unauthorised third-party access to reservation records. Criminals were already sending payment-redirection messages to those travellers almost immediately.

Carnival Corporation had the largest breach of the quarter. An attacker working under the ShinyHunters banner persuaded an employee to grant access to part of the corporate IT system. They reached about 8.7 million records with 7.5 million unique email addresses. The data was tied to the Holland America Mariner Society loyalty programme and covered names, dates of birth, gender, passport numbers and loyalty status. More than 800,000 residents of Texas alone received notification. The breach was detected on 14 April, and the notice followed on 27 May.

Qilin listed Avcon Jet in Austria on 4 June with sample files published. InterSPA-Gruppe in Germany was also listed during the June claim spree. An actor on a hacker forum offered material described as Ryanair legal claims platform data. This covered EU Regulation 261/2004 compensation cases, internal legal correspondence, flight data and banking details. No confirmation has followed.

SecureTrust research published in May 2026 found that 92% of travel agencies experienced a cyber threat in the previous twelve months. 66% reported customer data compromises. Cyberattacks were ranked as the leading threat to agency success by 68% of respondents, ahead of inflation and recession.

Data Assets at Risk

Data Asset	Detail and Q2 2026 Evidence
Passport and identity data	Passport numbers, dates of birth, gender, full names. Carnival Corporation. Approximately 8.7 million records taken through

Data Asset	Detail and Q2 2026 Evidence
	social engineering of an employee, with more than 800,000 Texans notified.
Loyalty programme records	Membership status, contact details, travel histories. Carnival. The Holland America Mariner Society programme held the affected records, and loyalty status was among the fields taken.
Reservation and itinerary data	Guest names, contact details, home addresses, booking dates and free-text notes. Booking.com. Reservation records used in payment-redirection phishing against travellers within days of the breach.
Corporate and legal records	Internal correspondence, claims data, banking details. Ryanair. Material offered on a hacker forum covering EU Regulation 261/2004 compensation cases, unconfirmed at the time of writing.
Operator and charter data	Client records, movement data, commercial documents. Avcon Jet. Sensitive data samples posted to the Qilin leak site on 4 June 2026.
RISK: HIGH Tourism operators hold the identity data that carries the heaviest regulatory weight and the itinerary data that makes downstream fraud convincing. The Q2 2026 evidence shows stolen reservation data reaching guests within days of a breach, which places the reputational consequence on the operator before its own investigation has concluded. International reach means notification obligations span several jurisdictions at once.	

6.4 Cross-Sector Observations

Three risks apply across all three sector categories and are worth naming for risk managers.

The platform holds the data and sets the risk

Across hotels, restaurants and tourism operators, Q2 2026 incidents repeatedly show that the compromised asset belonged to somebody else. Alsea's vendor, the Australian gaming supplier, Hotelogix, the shared European booking software and the Salesforce tenancies at Carnival, Aman Resorts and 7-Eleven are all cases where the victim had limited or no control over the system that failed. Vendor security assessment, contractual minimum standards and a documented inventory of who holds guest data on the organisation's behalf are baseline requirements, not governance enhancements.

Authentication answers who, and nothing else

The largest breach of the quarter began with an employee granting access to somebody who asked for it. Every technical control worked correctly at Carnival, because the identity presented was valid. Phishing-resistant standards such as FIDO2 and WebAuthn are still worth prioritising for administrative and privileged accounts. The Q2 evidence adds a second requirement. Monitoring has to cover what an identity does after it authenticates, specifically the volume and pattern of data it reads inside cloud platforms.

Dwell time is the unmanaged variable

BWH Hotels carried an intruder for six months. Carnival detected on 14 April and disclosed on 27 May. Neither organisation lacked security controls. Both were exposed by the gap between compromise and awareness, not by the initial failure. Logging of read activity on guest-facing applications and cloud platforms is the control that shortens that gap. It is routinely absent because those systems are monitored for uptime and revenue and not for unusual access.

7. Monetisation

This section examines how attackers converted Q2 2026 breaches into revenue across hotel, restaurant and food service, and tourism organisations. The mechanics of ransomware as a service, cryptocurrency settlement, leak site sequencing and post-breach remediation costs were set out in full in the Q1 2026 edition of this publication, available at https://www.uwl.ac.uk/sites/uwl/files/2026-06/Cyber_Risk_Resilience_Quarterly.pdf. This section covers only what changed during Q2 2026.

7.1 How Attackers Convert Breaches into Revenue

Three revenue models appeared this quarter that did not appear in Q1.

Extortion without encryption

The first is extortion without encryption, applied to data held in cloud platforms. ShinyHunters listed Aman Resorts and 7-Eleven on a pay-or-leak warning list on 18 April. The Aman claim covered more than 500,000 Salesforce records and carried a deadline of 21 April. No systems were locked and no operations were interrupted. The demand relies entirely on the threat to publish. This removes the victim's ability to recover through backups and reduces the decision to a question of when to disclose.

Extortion without intrusion

The second model dispenses with intrusion altogether. shadowbyt3$ found misconfigured cloud storage holding Hotelogix and Treebo guest folios, collected the data by simply requesting it, and attached a demand of 500,000 US dollars. The cost of the operation was the time taken to find the misconfiguration. When an attacker incurs almost no cost, the economics no longer require a large victim or a large payment. Small operators that previously fell below the threshold of commercial interest are now viable targets.

Leak site value

A third change concerns what the leak site itself is worth. Qilin posted eight sector victims across the quarter, three of them between 2 and 5 June. Most of them were small operators with no disclosed data volumes and no evidence of published data. A listing builds standing among affiliates whether or not it produces a payment. This means volume now carries value independent of extortion revenue.

7.2 Ransom Demands and Cryptocurrency

Only one demand figure was disclosed against a sector organisation during Q2 2026. This was the 500,000 US dollars attached to the Hotelogix and Treebo folio data by shadowbyt3$. No figure was disclosed for Carnival Corporation, Aman Resorts, 7-Eleven, Gelatissimo, Sysco, Mopaş Online Supermarket, or any of the eight Qilin listings.

In Q1 2026, the report recorded a demand of 1.5 million US dollars against Wynn Resorts and a demand of 5,000 US dollars against a Spanish municipal tourism operator. This gave a usable range. Q2 provides no such range.

The fact that no figures were disclosed is itself a finding. Groups running pay-or-leak campaigns against cloud platform data negotiate privately. They post deadlines, not amounts. This keeps the price flexible and denies analysts and insurers the benchmark data they need.

Risk managers who are pricing exposure or preparing a board position should treat published demand figures as a shrinking evidence base. They should rely on data volume, data category and regulatory jurisdiction as better predictors of the eventual cost.

7.3 The Decision to Pay or Refuse

Q2 2026 produced no publicly known payment or refusal outcome for any organisation in these sectors. No victim was removed from a leak site in circumstances that suggested a settlement. No group announced deletion of stolen data. No organisation stated that it had declined to engage.

Mopaş Online Supermarket confirmed the breach of its systems but did not comment on the demand. Gelatissimo confirmed only that an investigation was under way.

The Q1 2026 edition set out three contrasting outcomes at Washington Hotel, Wynn Resorts and Choice Hotels. That comparison remains the most useful available guide to the decision. Readers should refer to Section 7.3 of the Q1 edition.

What Q2 adds is a warning about the evidence base. Where every claim is unverified and no outcome is disclosed, an organisation preparing its own position cannot benchmark against peers. It must reason from its own data holdings, regulatory obligations and backup integrity instead.

7.4 Leak Site Pressure and Data Publication

Leak site activity during Q2 2026 shifted from pressure on individual victims towards competition between operators. NordStellar recorded 299 Qilin listings across the quarter against 284 for The Gentlemen. The Gentlemen rose 39% on Q1. Breachsense recorded The Gentlemen overtaking Qilin during June with 94 claimed victims. Qilin's sector activity fits that contest more closely than it fits any operational pattern.

Publication behaviour varied by group in a way that matters for verification. DragonForce published sample files from Gelatissimo covering employee records, financial information and internal documents. This substantiates the claim. Qilin listed Sysco with screenshots of alleged internal documents and posted sample files for Avcon Jet on 4 June. But it provided nothing for Jay's Catering, Don Don Group, InterSPA-Gruppe, Eat Salad or Sivatel Bangkok. Eleven of the twenty incidents rest on a claim with no independent verification and no victim statement.

For an organisation that appears on a leak site, the listing generates the same management time, media enquiries and partner questions whether or not any data was taken. The Q1 edition recorded the same effect through the contested Cl0p listing of Hilton Worldwide. A listing is a communications event before it is a security event. It needs a prepared response that does not depend on the technical investigation having concluded.

7.5 Loyalty Programme Exploitation

The Carnival Corporation breach is the clearest evidence yet that loyalty programmes are being targeted for the identity data they hold, not for points balances. The affected records were tied to the Holland America Mariner Society programme. They covered names, dates of birth, gender, passport numbers and loyalty status across about 8.7 million records with 7.5 million unique email addresses. Points theft did not feature. Passport numbers and dates of birth held alongside confirmed travel affiliation give an attacker everything needed for identity fraud and for social engineering that will remain credible for years.

Loyalty status is the field that deserves attention. A record that marks a member as high tier identifies a customer with disposable income, frequent travel and an established relationship with the brand. This makes that record more valuable per head than an ordinary customer record and makes the member a better target for a follow-up approach.

Loyalty databases held in cloud customer relationship platforms now carry the same exposure profile as the platform itself. The Aman Resorts listing suggests the same pattern applies to hotel loyalty data.

7.6 Insurance and Post Breach Costs

The cost profile of a Q2 2026 breach differs from Q1 in one important way. No incident this quarter produced a confirmed operational shutdown. No payment terminals were disabled. No ticketing or building systems were taken offline. Costs fell instead on notification, credit and identity monitoring, legal preparation and communications. Carnival Corporation notified more than 800,000 residents of Texas alone. This gives an indication of the scale involved before any regulatory or litigation cost is counted.

Dwell time has become the difficult variable for insurers. BWH Hotels carried an intruder from 14 October 2025 until 22 April 2026. This period spanned two calendar years and, for most organisations, two policy periods. Carnival detected on 14 April and disclosed on 27 May. Where the compromise predates the current policy and the claim arrives during it, the question of which policy responds is contested at exactly the moment the organisation needs certainty. The Q1 edition raised this in the context of delayed token exploitation. Q2 confirms the same problem arising from ordinary undetected intrusion.

Cloud storage misconfiguration raises a separate coverage question. The Hotelogix and Treebo exposure did not involve an intrusion, malicious code oro security failure in the usual sense. The storage was configured to permit access. Insurance policies that are designed to cover unauthorised access may not cover an incident where the victim's own settings allowed the access in the first place. Organisations should confirm with their broker how their policy treats misconfiguration. Hotels that rely on a property management vendor should establish whose policy responds when the vendor is the party that misconfigured the storage.

SecureTrust research published in May 2026 found that 92% of travel agencies experienced a cyber threat in the previous twelve months. 66% reported customer data compromises. Cyberattacks were ranked the leading threat to agency success by 68% of respondents, ahead of inflation and recession. Underwriters pricing this sector are working from a base rate that now approaches certainty. Organisations should expect renewal terms to reflect that and not to reward an absence of claims.

8. Legal, Regulatory and Litigation Landscape

The litigation patterns, the Japanese, UK and US regulatory positions, and the PCI DSS obligations that follow any cardholder data incident were set out in full in the Q1 2026 edition of this publication. Those positions have not changed and are not repeated here. This section covers what Q2 2026 adds, which is a wider set of jurisdictions, a set of disclosure timings that will bear on any future claim, and a new category of exposure arising from data held by vendors outside the organisation's control.

8.1 Litigation Trends

At the time of writing, no class action had been filed against any hotel, restaurant, food service or tourism organisation over a Q2 2026 breach. This is different from Q1 2026, when lawsuits against Panera Bread, Wynn Resorts and Choice Hotels were filed within weeks of the breaches becoming public. The difference is down to timing, not exposure. The Q2 breaches with the strongest claim profiles were disclosed late in the quarter, and the firms that monitor breaches usually take a few weeks to act.

Two cases stand out as the clearest exposure risks. Carnival Corporation confirmed about 8.7 million records, including names, dates of birth, gender, passport numbers and loyalty status. More than 800,000 residents of Texas alone were notified. The breach was detected on 14 April and the notice went out on 27 May. Any lawsuit will focus on whether the security controls in place before the intrusion were adequate, and whether six weeks between detection and notification was reasonable.

BWH Hotels disclosed on 11 May that an intruder had been inside its systems from 14 October 2025 until 22 April 2026. Six months of undetected access to guest reservation data is the fact a claimant firm will lead with. The organisation's defence will rest on what logging and monitoring existed on that application and whether it was proportionate to the data held.

Two Q1 attacks that only came to light during Q2 show the types of data that attract claims most reliably. RCI Internet Services notified 40,178 individuals about a breach involving names, Social Security numbers, driving licence numbers and passport numbers. Taos Mountain Casino sent out notifications about names, addresses and Social Security numbers after a DragonForce attack. Identity documents and government identifiers support a long-term identity fraud argument in a way that contact details alone do not.

What this means for your organisation. Detection and notification dates will be the first two facts examined in any claim, and both are established by your own records. Document what your monitoring covered, what it did not cover and why, before an incident forces you to reconstruct that reasoning under pressure.

8.2 Sector Regulatory Tracker

The Q2 2026 incident set spans a much wider range of countries than Q1. Several affected organisations would face simultaneous obligations under regimes with different thresholds, different clocks and different regulators. The points below describe the exposure created by the incidents in this report. They do not record any enforcement action, since none had been made public at the time of writing.

The Netherlands, Belgium and Ireland

More than 100 hotels lost reservation data in early June through what is believed to be a vulnerability in shared booking software. Reports came from all three countries. One flaw in one application creates parallel obligations under the General Data Protection Regulation to three national supervisory authorities, each with a 72-hour notification clock running from the moment the controller becomes aware. Every affected property is a controller in its own right, and none of them could detect the flaw or establish when the compromise began. When a shared platform fails, the notification burden falls on the businesses that used it, not on the vendor that built it.

Switzerland and the wider European set

Aman Resorts is based in Switzerland and falls under the revised Federal Act on Data Protection. This requires notification to the Federal Data Protection and Information Commissioner as soon as possible where a breach is likely to result in a high risk to the people concerned. InterSPA-Gruppe in Germany and Avcon Jet in Austria fall under the General Data Protection Regulation through their national authorities. Eat Salad in France falls under the same regime through the Commission Nationale de l'Informatique et des Libertés. Three of these four cases rest on an unverified leak site claim. This puts the organisation in the position of deciding whether an unsubstantiated assertion triggers a notification obligation.

Asia and the Pacific

Sivatel Bangkok falls under the Thai Personal Data Protection Act, which has a 72-hour notification requirement to the Personal Data Protection Committee. Hotelogix operates from Singapore under the Personal Data Protection Act, and Treebo from India under the Digital Personal Data Protection Act. The folio data exposed through misconfigured cloud storage belonged to hotels in several countries, which extends the obligation beyond the two vendors to their clients. Gelatissimo in Australia falls under the Notifiable Data Breaches scheme within the Privacy Act, with reporting to the Office of the Australian Information Commissioner. Mopaş Online Supermarket in Turkey falls under KVKK, the Turkish personal data protection law, and confirmed the breach after the leak site listing appeared.

United States

Carnival Corporation notified more than 800,000 residents of Texas alone. State-level notification obligations vary by threshold, timing and content across every state where affected individuals live. The Q1 2026 edition covers the federal position under the Cyber Incident Reporting for Critical Infrastructure Act and the state notification pattern established by the Wynn Resorts filing with the Maine Attorney General. Readers should refer to Section 8.2 of that edition. Passport numbers taken in the Carnival breach and Social Security numbers taken in the RCI Internet Services and Taos Mountain Casino breaches put all three in the categories that trigger the widest notification and remediation expectations.

What this means for your organisation. Map your notification obligations by jurisdiction before an incident forces you to do so under pressure. A single breach of a shared booking platform can trigger three regulators in Europe at the same time. A cruise or hotel group holding international guest records will face several more. Where your data sits with a vendor, establish now which party notifies, on what timetable, and who tells your guests.

8.3 Cyber Insurance

The insurance position we set out in the Q1 edition, covering things like phishing-resistant authentication, integration audits, identity theft cover and data separation, still applies. We are not repeating it here. Q2 adds three new points.

The first is dwell time. BWH Hotels had an intruder inside its systems from October 2025 to April 2026. That is two calendar years and, for most businesses, two policy periods. If the breach started before the current policy began but the claim comes in during it, the question of which policy pays out becomes a fight at exactly the wrong time. Organisations should check how their policy defines when an incident happens and whether past events are covered.

The second is cloud misconfiguration. The Hotelogix and Treebo exposure did not involve an intrusion. There was no malicious code, and no control was defeated. The storage was simply left open. A policy designed around unauthorised access may not pay out when the access was allowed by the insured's own settings, or by a vendor's. Hotels that rely on a property management vendor should find out whose policy responds when the vendor is the one who misconfigured the storage, and whether their own policy covers the notification costs that follow.

The third is the shift in costs. No Q2 incident caused a confirmed operational shutdown. The costs were all in notification, monitoring, legal advice and communications. Business interruption cover did not apply to any of these events. Organisations reviewing their limits should put more weight on privacy liability and notification cover, and less on interruption cover. This is the opposite of what the Q1 incidents would have suggested.

What this means for your organisation. Ask your broker three questions before renewal. How does the policy treat a breach that started in a previous policy period? Does it cover a cloud storage misconfiguration where there was no unauthorised access? Are notification and legal costs covered at a limit that matches the number of people in your guest and employee records, rather than the size of your IT estate?

9. Threat Outlook

This section looks ahead to the rest of 2026 and into early 2027. Each assessment covers a threat area we have seen in this report and comes with a confidence rating. These ratings reflect how strong the evidence is and how much agreement there is among analysts.

High confidence means the assessment is backed by multiple independent sources and consistent patterns of behaviour. Moderate confidence means the evidence is credible but has gaps or limited corroboration. Low confidence means the assessment is plausible but based on limited or indirect evidence.

9.1 Ransomware and Data Extortion

Confidence level: High. Ransomware groups will keep targeting hotels, restaurants, food service and tourism businesses through the rest of 2026, with food service taking the biggest hit. Ten of the twenty incidents this quarter involved ransomware, and food and beverage companies had the sharpest rise at 80% month on month in May. Qilin listed eight sector victims, and DragonForce, AUDIT TEAM and shadowbyt3$ each added more claims. Verizon's 2026 Data Breach Investigations Report found that ransomware accounted for 48% of all data breaches globally.

The model that will grow fastest is extortion without encryption. The Aman Resorts and Hotelogix cases show that attackers can issue a demand against data alone at almost no cost to themselves. This removes the protection that tested backups would otherwise provide.

9.2 Identity and Credential Exploitation

Confidence level: High. Compromise of cloud customer relationship platforms through social engineering will remain the method that produces the largest single breaches across all four sectors. Carnival Corporation, Aman Resorts and 7-Eleven were all hit through Salesforce environments within a fortnight in April. The Carnival case came down to an employee granting access, not a technical failure.

Guest, loyalty and marketing data has moved to platforms that check identity but monitor nothing beyond that. This trend will continue. Organisations that hold guest data in Salesforce, Zendesk, Snowflake or similar platforms without session monitoring and anomaly detection on data volume remain exposed, no matter how strong their authentication controls are.

9.3 Third Party and Supply Chain Risk

Confidence level: High. Attacks and failures involving third-party vendors, shared software and vendor-operated cloud storage will increase in frequency and impact. Four of the twenty Q2 incidents relied on a third party. The multi-country European booking software breach reached more than 100 independent hotels across three jurisdictions through a single flaw that none of them could patch.

Alsea lost 12.6 GB, including plaintext credentials, through a vendor with no breach of its own systems. Hotelogix and Treebo lost guest folios through misconfigured cloud storage. Qilin listed an Australian hospitality and gaming technology supplier that serves downstream operators.

The sector is becoming more concentrated on a small number of property management, booking and payment platforms. This means any single vendor failure will expose more organisations.

9.4 Social Engineering Targeting Sector Staff

Confidence level: High. Phishing campaigns against front desk, reservations and administrative staff will continue and will increasingly come through legitimate services. The campaign Microsoft disclosed on 25 June sends messages through Calendly notification infrastructure, a technique Microsoft called

authentication laundering. These messages pass SPF and DKIM checks because the sending domain is genuine.

Check Point found more than 210 sequentially numbered hotel-lure domains alongside Booking.com and Airbnb impersonation clusters in April and May. Sending reputation, which is what most email filtering relies on, does not stop a message from a service the organisation already allows. Now that the technique has been documented, other criminal groups will adopt it.

9.5 Infostealers and Malware

Confidence level: Moderate. Malware in these sectors will continue to move away from file-based payloads towards memory-resident implants that leave nothing for a scanner to find. The Node.js implant used in the hotel campaign runs entirely in memory and sends signals over non-standard ports. The compromised machines Microsoft identified were front-office workstations that hold live sessions into property management, payment and reservation systems.

No infostealer family was named in sector incidents during Q2 2026, which is a change from Q1. This is why the confidence is moderate rather than high. The underlying market for stolen credentials has not shrunk. The absence of named families this quarter is more likely about how incidents were reported than about any change in attacker behaviour.

9.6 Regulatory and Litigation Pressure

Confidence level: Moderate. Regulatory and civil exposure from Q2 2026 incidents will become clear over the next two quarters, not immediately. At the time of writing, no class action had been filed against a sector organisation over a Q2 breach, and no regulator had announced an investigation. This is why the confidence is moderate.

The conditions are there. Carnival notified more than 800,000 residents of Texas alone after a breach involving passport numbers and dates of birth. BWH Hotels disclosed six months of undetected access. The Q1 attacks that became public during Q2 involved Social Security numbers, driving licence numbers and passport numbers. The wider spread of jurisdictions this quarter, covering the Netherlands, Belgium, Ireland, Switzerland, Germany, Austria, France, Turkey, Thailand, Singapore, India, Australia and the United States, means any organisation caught in a shared platform failure faces several regulators at once.

9.7 Operational Technology and Physical Systems

Confidence level: Low. Attackers could still go after operational systems like payment terminals or building controls, but there was no evidence of it this quarter. Q2 2026 had no confirmed disruption to payment terminals, ticketing systems, access control or building management anywhere in the sector. That is a big change from Q1 2026, when four organisations lost operational systems.

The underlying risks have not changed. Hotels still run property management, point of sale, access control and building systems on connected networks that are often hard to patch. The front-office machines that Microsoft identified as compromised this quarter had live connections to payment systems, but there was no reported disruption. This suggests attackers reached those systems and chose to take the data and leave the systems alone.

The confidence level has been dropped from moderate to low because no actual incident was observed this quarter. This should be read as a comment on what attackers chose to do and not as a sign that the risk has gone away.

9.8 Insider Threats

Confidence level: Moderate. The risk of an insider helping an attacker will stay relevant, and the line between a genuine insider and an employee who has been tricked is getting harder to see. The Carnival breach started with an employee giving access to someone who asked for it. That achieved the same result as a paid insider, without any payment or existing relationship.

Hotels, restaurants and food service businesses employ lots of people who have access to guest data and payment systems. High staff turnover, seasonal hiring and a culture that rewards helpfulness all play into the attacker's hands.

There was no direct evidence of paid insider recruitment in these sectors during Q2 2026. The confidence rating reflects that gap, not a belief that the risk has gone down.

9.9 Monetisation and Dark Web Activity

Confidence level: High. Leak sites and underground markets will stay the main channels for extortion and for selling guest data. The number of claims will keep rising faster than the number of confirmed compromises. NordStellar recorded 299 Qilin listings this quarter against 284 for The Gentlemen, which was up 39% on Q1. Breachsense recorded The Gentlemen overtaking Qilin in June with 94 claimed victims. Eleven of the twenty incidents in this report are based on a claim alone.

Guest data that includes passport numbers, loyalty status and future bookings is particularly valuable. It enables fraud that looks genuine to the person receiving it. The Booking.com case shows that value being realised within days of the theft. Organisations that do not monitor for their own data on these sites will find out about it from a guest or a journalist.

Assessment Summary

The evidence from Q2 2026 shows hotels, restaurants, food service and tourism organisations facing a threat environment shaped by three things. Extortion based on data held outside the organisation. Identity compromise inside cloud platforms. And failures in shared software and vendor infrastructure that individual operators cannot detect or fix.

The highest confidence assessments are for ransomware and data extortion, identity exploitation, third-party risk, social engineering and dark web monetisation. Moderate confidence assessments apply to malware evolution, regulatory and litigation pressure and insider threats. In these areas, the conditions are there but the Q2 evidence is thin.

Operational technology is rated low confidence after a quarter with no observed disruption. This should be read as a comment on what attackers chose to do, not as a sign that the underlying risk has gone away.

These assessments should inform security investment and business continuity planning for the rest of 2026 and into 2027.

10. Recommendations

The recommendations here come from the incidents, attack methods and defensive failures we have covered in Sections 1 through 8. Each one is based on what went wrong in Q2 2026 and what would have made a difference. Alongside these incident-specific measures, each section also includes basic practices that are always worth doing, no matter what the current threat landscape looks like.

10.1 Identity Governance and SaaS Visibility

Carnival Corporation, Aman Resorts and 7-Eleven were all hit through their Salesforce environments in April 2026. In Carnival's case, an employee gave access to someone who asked for it. Every authentication control worked as it should, because the identity was valid. Authentication told you who logged in. Nothing told you that the same identity then read about 8.7 million records.

If your organisation holds guest, loyalty or marketing data in Salesforce, Zendesk, Snowflake or a similar platform, you should turn on data access logging inside that platform. Set up alerts for export and bulk read volumes that are out of line with normal business use. A staff member who usually reads a few hundred records a day and suddenly reads several hundred thousand in one afternoon is exactly the signal that would have shortened every one of these breaches. The logging is already available inside the platform at no extra cost.

Beyond that, you should keep a documented list of every cloud platform that holds personal data. Note who administers it, which systems connect to it and what each connection is allowed to read. Many hotel and restaurant groups have connections to booking engines, loyalty systems and marketing tools that were set up years ago and never reviewed. Each of those still has standing access.

These measures sit alongside the basics of identity governance. Apply least privilege to user and service accounts. Restrict administrative credentials to named administrators. Get rid of shared accounts. Review access at set intervals. Disable any account belonging to a former employee or a vendor you no longer use and do it immediately.

What this means for your organisation. Find out today whether anyone in your organisation would be alerted if a single account exported your entire guest database from your CRM. If the answer is no, or if nobody is sure, that is the first gap to close. It costs configuration time, not money.

10.2 Behavioural and Network Monitoring

The malware used in the hotel phishing campaign is written in Node.js. It runs entirely in memory and writes nothing to the file system. Antivirus and endpoint tools that scan files will find nothing, because there is no file to scan. The malware stays active through the live session and through repeated delivery to the same reception mailboxes. It does not rely on a startup folder entry or a registry key that endpoint tools are set up to watch.

Detection has to happen on the network. Compromised machines send signals to command-and-control systems for unusual ports. A front-desk workstation has a narrow and predictable traffic pattern, which makes unusual outbound connections easier to spot. Security teams should establish what normal outbound traffic looks like for front-office terminals and set-up alerts for anything that deviates from that. This monitoring should also cover franchise and remote properties, where coverage is often weakest.

Microsoft identified the compromised machines by their device names, which included reception, frontdesk, reservations, accueil and recepce. Use that naming convention as a way to keep track of your machines, not as a problem. You should be able to produce a list of every machine that handles front-office work, what it connects to and when it was last patched.

These detection measures rely on a basic foundation. Keep endpoint protection up to date with current signatures. Patch operating systems and applications regularly. Make sure every device on the network is covered, including back-of-house terminals that are often overlooked in hotels and restaurants.

What this means for your organisation. Ask your security team whether an outbound connection from a front-desk terminal to an unknown address on an unusual port would trigger an alert tomorrow. File-based detection will not catch this kind of attack. The network is the only place you will see it.

10.3 Phishing and Authentication Countermeasures

The campaign that ran from April 2026 sends phishing messages through Calendly notification infrastructure. Microsoft named the technique “authentication laundering” when it disclosed the campaign on 25 June. Messages sent this way pass SPF and DKIM checks and carry a clean reputation because the sending service is genuine. There is no filter rule based on sender reputation that can separate these messages from the legitimate notifications that arrive alongside them.

Staff training is the first line of defence and needs to be specific. Guidance to avoid suspicious senders is actively misleading against this technique. Train front desk, reservations and complaints staff on one key principle: a message from a trusted service still needs its content verified. Any request to run a command, install software, open an unexpected attachment or log in through an embedded link should be checked through a separate known channel, no matter who appears to have sent it.

On the technical side, restrict PowerShell and script execution on front-office terminals where they are not needed for operational purposes. Apply application control so only approved software can run. Consider blocking scripting runtimes on machines that have no development function. Check Point identified more than 210 sequentially numbered hotel-lure domains along with Booking.com and Airbnb impersonation clusters in April and May. This means you should watch for newly registered domains that mimic your brand and request their removal as soon as possible.

The Carnival breach started with a conversation and not an email. The countermeasure is procedural. Verification steps for access requests need to be specific enough that a staff member can turn down a plausible request without feeling obstructive. The procedure also has to work during a busy shift, with a new starter and with a caller who sounds senior.

For administrative and privileged accounts, phishing-resistant authentication using FIDO2 or WebAuthn hardware keys is still the strongest protection you can put in place. Make it a priority for anyone with platform administration rights.

What this means for your organisation. Run a test. Send a simulated notification from a service your staff already trust and see how many follow the instructions. Then check that your front-office terminals cannot run scripts they do not need. Make sure a member of your reservations team knows exactly what to do when a caller asks for access.

10.4 External Exposure, Cloud Configuration and Dark Web Monitoring

Hotelogix and Treebo lost guest folios because their cloud storage was left open to the public. Nobody hacked in. No security control failed. No alert went off. The data was simply there for the asking. Storage permissions tend to be set once when something is first deployed, then rarely looked at again. They are often left out of penetration tests that focus on network infrastructure.

You should audit every cloud storage container that holds personal data. Check that public access is off and that access logging is on. Do this on a regular schedule, not just when you set something new up. If you use a property management, booking or loyalty vendor to hold guest data on your behalf, your contract should require evidence that they do the same kind of audit. You carry the notification obligation if something goes wrong. The vendor holds the configuration that determines whether it does.

The Booking.com breach and the multi-country European breach both led to guest-directed fraud within days of the theft. This means dark web monitoring has a shorter useful window, but it still matters. Keep monitoring your corporate domains, employee email addresses and integration credentials. Also watch for your own guest data appearing in circulation. In both of those cases, the first sign of trouble came through customers, not through monitoring.

BWH Hotels traced its breach to a flaw in a guest-facing web application that gave attackers access for six months. External vulnerability assessments and a full list of your internet-facing assets, including old applications that teams have deprioritised, would have shortened that window.

These monitoring measures work best when your attack surface is small. Limit what you expose to the internet. Close unused ports and services. Provide remote access only through a VPN. Put web-facing applications behind a web application firewall.

What this means for your organisation. Make a list of every cloud storage location that holds guest data, including those run by your vendors. For each one, confirm whether public access is off and whether read activity is logged. If you cannot make that list, the Hotelogix outcome is available to your organisation on the same terms.

10.5 Tabletop Exercise Scenarios for Hotel, Restaurant and Tourism Environments

The incidents in this report can be used as ready-made scenarios for tabletop exercises. These exercises can test how well your incident response team would handle a real attack. The scenarios below are designed for cross-functional teams that include IT, operations, legal, communications and senior management.

Scenario 1. Social engineering of a cloud platform (Carnival Corporation)

An employee gets a believable request and gives a caller access to part of the corporate IT system. Six weeks later, the organisation finds out that several million guest records, including passport numbers and dates of birth, were read from its CRM platform. This exercise tests whether the team can work out what was accessed using platform logs, decide on a defensible detection date, set a notification timeline across different countries, and explain to the board why all the technical controls were working perfectly the whole time.

Scenario 2. Phishing from a trusted service (authentication laundering campaign)

A reservations team member opens a meeting notification from a scheduling service that the organisation uses every day. The message passes every filter. Within minutes, a memory-resident implant is running on a front-desk terminal that has an active session into the property management system. This exercise tests whether the team can spot the breach through network activity, since file scanning will find nothing. They also need to isolate a terminal that reception relies on during service hours, assess whether the property management system was accessed, and report to the relevant data protection authority.

Scenario 3. Shared booking software failure (Netherlands, Belgium and Ireland)

A hotel finds out from a guest that cybercriminals are sending payment demands quoting real reservations. The hotel has no evidence of a breach in its own systems. Reports start coming in that properties in two other countries are affected too. This exercise tests whether the team can act without confirmed technical proof, get information from a vendor that has not yet admitted there is a problem, warn guests before they fall for the fraud, and decide whether they have a legal duty to notify anyone when they cannot even establish when the compromise happened.

Scenario 4. Cloud storage exposure at a vendor (Hotelogix and Treebo)

A property management vendor discloses that guest folios, stay details and partial payment card data held on its cloud storage were left open to the public. A third party collected the data and is now demanding

payment. This exercise tests whether the team can work out which guests are affected, figure out whose insurance covers the incident, agree with the vendor on who notifies guests and when, and respond to a guest who wants to know why the hotel let a third party hold their personal information in the first place.

Scenario 5. Unverified leak site listing (Qilin claim spree)

The organisation appears on a ransomware group's leak site with a threat to publish data unless negotiations start. No data samples are provided. No systems are encrypted. No anomalies show up in the logs. The claim cannot be confirmed or ruled out. Media enquiries start within hours.

This exercise tests whether the team can respond publicly while the investigation is still open, decide if an unverified claim triggers a legal duty to notify anyone, handle questions from partners and franchisees, and hold their ground under commercial pressure to make the story go away.

Run each scenario with defined roles, a time limit of no more than two hours, and a structured debrief that produces a written action list with owners and deadlines. Repeat the scenarios at least once a year, and update them to reflect the latest threat intelligence.

The organisation appears on a ransomware group leak site with a threat to publish unless negotiations

Appendix A. Full Incident Matrix

Every Q2 2026 incident and the two Q1 attacks disclosed during the quarter, mapped against the five stages of a typical cyber intrusion described in Section 2. Where the public record does not establish a stage, the cell records that the information was not reported. Leak site listing dates are not intrusion dates, and eleven of the twenty in-scope incidents rest on a criminal claim alone.

Organisation	Sub-sector	Initial Access (how they got in)	Execution and Persistence (what ran, how they stayed)	Credential Access and Evasion (logins, hiding)	Collection and Exfiltration (what was taken)	Impact (what it cost)
April 2026						
Booking.com (NL)	Tourism and Travel	Unauthorised third-party access to reservation data; vector not disclosed	Not reported	No group claimed the incident	Guest names, email addresses, telephone numbers, home addresses, booking dates, free-text notes to hotels	Customers notified 12 and 13 April; data reused within days in payment-redirection phishing
Carnival Corporation (USA)	Tourism and Travel	Social engineering of an employee granting access to part of the IT estate (ShinyHunters)	Valid session inside the Salesforce environment; no malware deployed	Legitimate identity; activity appeared normal to monitoring	Approximately 8.7 million records, 7.5 million unique emails; names, dates of birth, gender, passport numbers, loyalty status	Detected 14 April, disclosed 27 May; more than 800,000 Texas residents notified
Aman Resorts (CH)	Hotel	Salesforce environment compromise (ShinyHunters)	Not reported	Valid identity to a cloud platform	More than 500,000 records claimed, holding personal data	Pay-or-leak listing 18 April, deadline 21 April; unverified
BWH Hotels (Best Western, WorldHotels, Sure Hotels)	Hotel	Flaw in a web application holding guest reservation data	Access ran 14 October 2025 to 22 April 2026, six months undetected	Read activity not logged; dwell time established by inference	Guest names, contact details, home addresses, reservation numbers, dates of stay, special requests; payment data held separately and unaffected	Disclosed 11 May; privacy exposure without financial loss
Ryanair (IE)	Tourism and Travel	Not established; material offered on a hacker forum	Not reported	Unattributed forum actor	Alleged legal claims platform data covering EU Regulation 261/2004 cases, internal correspondence, flight data, banking details	Unconfirmed; no confirmation followed
7-Eleven	Restaurant and Food Service	Salesforce environment compromise (ShinyHunters)	Not reported	Valid identity to a cloud platform	Data categories not detailed	Named on the 18 April pay-or-leak list; unverified
Alsea (Domino's, Starbucks, Vips operator, LatAm)	Restaurant and Food Service	Third-party technology vendor compromised; no breach of Alsea systems	Not reported	Plaintext credentials exposed in the vendor environment	12.6 GB including plaintext credentials, transaction records, audit reports, live surveillance camera access	Alsea named among affected clients
Hotels across Europe and Asia (unnamed)	Hotel	Phishing routed through Calendly notification infrastructure (authentication laundering)	Memory-only Node.js implant; persistence from the live session and repeated delivery to reception mailboxes	Passes SPF and DKIM; genuine sending domain; runs in memory with no file on disk	Beaconing over non-standard ports; sessions into property management, payment and reservation systems	Front-office workstations compromised; Microsoft disclosure 25 June; active and ongoing
Hotelogix and Treebo Hotels (SG/IN)	Sector Technology	Misconfigured Amazon S3 buckets and Azure blob storage	No intrusion; data collected by bulk scraping	No control defeated; generates no intrusion alert	Guest folios, contact details, arrival and departure dates, room numbers,	USD 500,000 demand (shadowbyt3$)

Organisation	Sub-sector	Initial Access (how they got in)	Execution and Persistence (what ran, how they stayed)	Credential Access and Evasion (logins, hiding)	Collection and Exfiltration (what was taken)	Impact (what it cost)
		permitting access without authentication			partial card and transaction data	
Gelatissimo (AU)	Restaurant and Food Service	Not disclosed	Ransomware with exfiltration (DragonForce)	Not reported	352 GB claimed; sample files covering employee records, financial information, internal documents	Investigation acknowledged; sample files published
May 2026						
Sysco (USA)	Restaurant and Food Service	Not disclosed	Ransomware and data extortion (Qilin)	Not reported	Screenshots of alleged internal documents	Leak site listing, negotiation deadline 12 May; no operational impact disclosed
Australian hospitality and gaming IT supplier	Sector Technology	Not disclosed	Ransomware (Qilin), 15 May	Not reported	Not disclosed	Leak site listing; downstream hospitality and gaming customers potentially exposed
Mopaş Online Supermarket (TR)	Restaurant and Food Service	Not disclosed	Ransomware and leak site extortion (AUDIT TEAM)	Not reported	Not disclosed	Breach of systems confirmed by the company after the listing appeared
June 2026						
More than 100 hotels (NL/BE/IE)	Hotel	Probable vulnerability in shared hotel booking software	Properties could not detect or patch the flaw	Not reported	Customer and reservation data	Data reused in phishing demanding payment under threat of cancellation; more than 100 properties across three countries
Jay's Catering (USA)	Restaurant and Food Service	Not disclosed	Ransomware (Qilin), 2 to 5 June claim spree	Not reported	Data categories not disclosed	Leak site listing; unverified
Don Don Group	Restaurant and Food Service	Not disclosed	Ransomware (Qilin), 2 to 5 June claim spree	Not reported	Data categories not disclosed	Leak site listing; unverified
InterSPA-Gruppe (DE)	Tourism and Travel	Not disclosed	Ransomware (Qilin), 2 to 5 June claim spree	Not reported	Data categories not disclosed	Leak site listing; unverified
Eat Salad (FR)	Restaurant and Food Service	Not disclosed	Ransomware and data extortion (Qilin), 3 June	Not reported	Data volume and categories under investigation	Threat to publish unless negotiations commence
Avcon Jet (AT)	Tourism and Travel	Not disclosed	Ransomware and data extortion (Qilin), 4 June	Not reported	Sensitive data samples posted to the leak site	Threat to publish; sample files published 4 June
Sivatel Bangkok (TH)	Hotel	Not disclosed	Ransomware and data extortion (Qilin), 21 June	Not reported	Sensitive data claimed	Threat to publish unless negotiations commence
Q1 2026 Attacks Disclosed During Q2 2026						
Taos Mountain Casino (USA)	Tourism and Travel	Not disclosed	Ransomware with exfiltration (DragonForce), March	Not reported	Names, addresses and Social Security numbers; 38.6 GB claimed	Notifications issued during Q2
RCI Internet Services (USA)	Sector Technology	Unauthorised system access, March	Not reported	Not reported	40,178 individuals; names, Social Security numbers, driving licence numbers, passport numbers	Notifications issued during Q2

Contact

Prof Alexandros Paraskevas (PhD)
Director of the International Centre for Hospitality and Aviation Resilience Management (ICHARM)
Professor in Strategic Risk Management
Chair of Hospitality Management and Doctoral Programmes Lead

London Geller College of Hospitality and Tourism
University of West London | St. Mary's Road, Ealing, London W5 5RF, United Kingdom

Direct Line +44 (0)20 8231 2279
Mobile +44 (0)779 382 2593
E-mail Alexandros.Paraskevas@uwl.ac.uk
Website uwl.ac.uk/users/alexandros-paraskevas

ICHARM

The International Centre for Hospitality and Aviation Resilience Management (ICHARM) at the University of West London focuses on risk, resilience, and performance in hotels, restaurants, and tourism organisations. The team brings together hospitality, cyber security, and legal expertise to support boards and senior managers in service based businesses.

The ICHARM Cyber Threat Intelligence team tracks attack patterns, threat actors, and legal outcomes that affect hotels, restaurant and food service operators, tourism brands, and their technology providers. It uses regulatory filings, incident reports, dark web and open source monitoring, and sector specific threat feeds to build an evidence base for decision making in hospitality and tourism.