DATA DISTURBANCE

With high-profile data breaches in the travel industry hitting the news in recent years, *BBT* finds some troubling details about business travellers and cyber security

3 in 10

senior business managers have been hit by cybercrime while abroad

SOURCE: KASPERSKY LAB

POINTING FINGERS

Those who travel for work feel it's their employers' responsibility to handle data security while they're overseas

SOURCE: KASPERSKY LAB

47%
believe employers should accept security risks when sending staff abroad

41%
expect their employers to have strong security measures in place

27%
have used a work device to access online banking via wifi

20%
admit to using work devices to access websites of a sensitive nature via wifi

in association with HRS Global Hotel Solutions

WIFI RISK

A survey of 11,850 people around the world revealed the biggest threat to company data is business travellers

59% in senior roles log on as soon as they can upon arrival

48% of senior managers use unsecured public wifi networks to connect their work devices abroad

44% use wifi to transmit work emails with sensitive or confidential attachments

SOURCE: KASPERSKY LAB

51.2% OF EMPLOYEES ACKNOWLEDGE THAT THERE ARE GUIDELINES IN PLACE FOR USING WORK DEVICES OUTSIDE OF THE OFFICE

SOURCE: OBSERVEIT

TENSE TRAVELLERS

According to a survey of 2,000 business travellers, 35 per cent are nervous about compromising their employer's data safety while travelling. When asked what they worry about, they said:

Having their laptop or mobile device stolen or lost	29%
Using public wifi	21%
Working on their laptop or mobile	9%
Unintentionally sharing company documents	9%
Accessing company emails	8%
Opening a file or visiting a website they shouldn't have	8%
Disposing of paper documents	6%

SOURCE: CARLSON WAGONLIT TRAVEL

HOLIDAY HAZARDS

A survey of 1,000 US-based employees found many could be exposing company data during their holidays

53% ANTICIPATE NEEDING TO BRING A WORK DEVICE ON HOLIDAY

77% USE FREE/UNSECURED WIFI USING A WORK COMPUTER OR PHONE WHILE TRAVELLING

63% USE FREE/UNSECURED WIFI TO CHECK WORK EMAILS OR ACCESS FILES

54% USE UNSANCTIONED PERSONAL DEVICES TO CHECK WORK EMAILS

55% USE A SECURE VIRTUAL PRIVATE NETWORK (VPN) TO ACCESS WORK EMAIL AND FILES WHILE WORKING REMOTELY

21% LEAVE THEIR WORK DEVICES UNATTENDED WHILE TRAVELLING

SOURCE: OBSERVEIT

28% of travel managers look to their TMC to protect their travellers' personal data

SOURCE: ABTA

TRAVEL INDUSTRY DATA BREACHES IN NUMBERS

Company name	Year	Data breach
Marriott International/ Starwood	2014-18	Up to 500 million guests (327 million included a combination of name, address, passport number and check-in information)
Cathay Pacific	2018	Up to 9.4 million passengers, including passport numbers, email addresses and some credit card details
Uber	2016	Up to 57 million customers and drivers
British Airways	2018	Up to 380,000 transactions, as well as 77,000 customers' payment card details
ABTA website	2017	Up to 43,000 users
Air Canada	2018	Up to 20,000 mobile+ app users
IHG	2016	Data from 1,200 properties, including cardholder names, numbers, expiration dates and internal verification codes
Hyatt	2015	Malware in payment systems of 318 hotels
Singapore Airlines	2019	285 Krisflyer members
Hyatt	2015	200 Gold Passport members
Mandarin Oriental	2014-15	Security breach at 10 hotels
Eurostar	2018	Unspecified
Hilton	2014-15	Unspecified

SOURCE: VARIOUS

TIPS FOR TRAVELLERS TO MITIGATE CYBER RISK WHILE ON THE ROAD

- **Turn off** or lock devices at airport security
- **Avoid accessing** sensitive data on public networks
- **Disable Bluetooth** and wifi on work devices when not in use
- **Create a personal** hotspot with your smartphone and use a VPN to encrypt data
- **Assume conference room** microphones, telephones and video conferencing equipment are compromised
- **Take as few devices** with you as possible and never leave them unattended
- **Charge devices** using only regular power outlets or your own battery-powered charging device
- **If you have to use** a USB outlet at a charging station, power off the device before plugging in
- **Don't use devices** offered to you by a third party and don't let anyone else use your device
- **Don't download** software on to your devices during your trip and have your IT team do a security check when you return
- **Assume any device** screened at border controls has been exploited

SOURCE: FCM TRAVEL SOLUTIONS

59% of senior managers feel there's an expectation from their employer to stay connected when travelling for work

SOURCE: KASPERSKY LAB