Data security, Covid-19 and the hotel sector

By Kate Brimsted, UK head of data privacy and cyber security at Bryan Cave Leighton Paisner LLP

by HEATHER SANDLIN — Friday, 18 September 2020, 10:28 *in* **Coronavirus**, **Features** Reading Time: 4 min

kate-brimstead

As the UK's 3rd biggest employer in 2017 according to UK Hospitality, the economic importance of reopening the UK's hospitality sector cannot be overstated. Add to this, the weary toll taken by isolation and monotonous home catering, and many guests as well as staff are eager to see this vibrant industry get back to strength.

However, as well as guarding against the risks to health from Coronavirus, hotel and restaurant owners also need to pay attention to increased data security risks. The sector's role in support of the government's Test and Trace service inevitably increases the quantity of personal data held about guests/diners. The pandemic has also radically disrupted established ways of working and of interacting with each other. For those sectors capable of continuing to function during the lockdown, adjusting to a 100% home working environment and reduced live contact with colleagues has been a rich breeding ground for scammers using phishing emails and "low tech" methods like social engineering to perpetrate bank transfer frauds and identity theft. Not all data compromise incidents are the result of malicious third parties; accidental error and carelessness continue to play a part (including the security "workaround" by the frustrated home worker struggling with an unfamiliar IT set up).

Wherever there is a pool of personal data, this presents criminals with an opportunity. It is worth keeping in mind that even seemingly innocuous items of information can be combined with other information obtained by scammers to considerable effect. The more prestigious the establishment, the greater the potential presented by its affluent clientele. The recent incident at the Ritz reportedly involved unauthorised access to the food and beverage ordering system. Criminals then

apparently spoofed the hotel's phone number and called future guests, claiming their credit card had been declined and requesting new card details to guarantee their booking. The fact that the scammers knew the dates and details of the booking, may well have helped convince a number of guests that the call was genuine.

To paraphrase a popular quote, there are only two types of organisations: those which know they have had a security breach and those which don't realise it yet. The hotel sector is no exception and therefore with cyber attacks on the rise, as well as regulatory fines (see below), what should management teams be doing to fortify their data protection governance?

Some priorities will depend on your specific IT environment, e.g. hosting, extent of interaction and connectivity with third party systems, software applications, operating system, volume and type of data (especially payment card industry requirements, if applicable). However, many aspects are common across a range of set ups, such as assigning responsibility for GDPR compliance within the organisation, resourcing the role appropriately and ensuring a reporting line to the board. Providing data protection training that is role-appropriate is increasingly important; encourage staff to treat every piece of guest data as valuable – that booking detail could be the final piece of the jigsaw for a fraudster to pull off a bigger theft, e.g. to persuade the customer that they are calling from their bank's fraud department and take over the account.

Other steps include revoking IT system access for departing or furloughed staff, and ensuring access to booking systems is limited to persons who need it for their roles, with complex passwords required to be changed regularly. Establishments looking to introduce COVID-friendly remote payment systems for restaurant guests will want to ensure that these third party apps are robust from a data security perspective, so that the customer's data and their payments are assured.

What are the potential sanctions where data incidents occur? As well as fines of a maximum of 4% of annual global turnover or £17 million (whichever is higher), orders mandating changes to data use, even the deletion of data, can be issued by the UK's data protection regulator, the ICO.

The ICO announced in June 2019 it was intending to fine Marriott Hotels £99.2m following a long-running, historic data breach affecting 30 million EU citizens and linked to the Starwood hotels group acquisition in 2016. The compromised data included credit card details, passport numbers and the dates of birth of some guests. Marriott has appealed and the size of the final fine is expected to be lower and to be known in the next couple of months. In addition, there is a growing trend in the UK of group litigation seeking compensation being brought by individuals affected by data security breaches. It was announced in August that one such group claim is being brought against Marriott in the High Court in London; the representative class is expected to include several million individuals, meaning that even a modest individual amount could equate to a very substantial overall figure.

An ounce of prevention is worth a pound of cure. Learning from the misfortunes of others through data security training, and mock data breach exercises, helps bring the risks to life. Firms like BCLP often work with clients in this sector, devising bespoke education and data breach incident "drills". Employees can often be identified as a vulnerability when it comes to data protection; at the same time they can also be seen as the gate keepers of an organisation's data security and also of its reputation – surely worth an "ounce" of investment.

By Kate Brimsted, UK head of data privacy and cyber security at Bryan Cave Leighton Paisner LLP

Leave a Reply

Enter your comment here...

CORONAVIRUS

Data security, Covid-19 and the hotel sector

BY HEATHER SANDLIN Friday, 18 September 2020, 10:28

CORONAVIRUS

Cumbrian tourism business confidence 'plummets', study finds

BY MEGAN SMITH Friday, 18 September 2020, 10:02

Beannchor Group opens new £4m Haslem Hotel

Friday, 18 September 2020, 11:30

Mayor of London urges government to extend business rates holiday

Friday, 18 September 2020, 11:07

Cumbrian tourism business confidence 'plummets', study finds

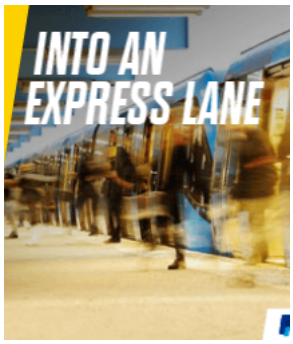
Friday, 18 September 2020, 10:02

York guest house bought by first-time buyers

Friday, 18 September 2020, 9:43

Former House of Fraser store to become 'boutique' hotel

Friday, 18 September 2020, 8:50



CATEGORIES

Advice Angie Petkovic Appointments Business Bites Columns Concepts Coronavirus Coronavirus Coronavirus Current Affairs Economy Editor's Blog Events Features Free to read Front of House Hotel Brands Hotel Concept of the Month Hotels Latest News Opinion People Profiles Interviews Property Regulation Restaurants & Chefs Special Coverage Sponsored Stephen Ayers Technology Tech Talk The Project Tips Tourism Trade Organisations Uncategorized

OTHER MULBERRY BRANDS

Jewellery Focus
Pet Gazette
Retail Sector
Funeral Service Times
Catering Today
Accountancy Today
Insurance Wire
Banking Sector
Media Sector