Data Risk in the Post GDPR Landscape

Jonathan Harrison
Henderson Insurance Brokers Ltd, an AON Company

Contents

1. “We’re all going to have to change how we think about data protection” 5
2. 18 Months of GDPR 6
3. ICO – fines, penalties and more 9
4. Company impact – the effects of GDPR 10
5. Mapping the GDPR landscape – mitigating future risk 12

“We’re all going to have to change how we think about data protection”

By including this comment in her speech to the Institute of Chartered Accountants in England and Wales in London on 17th January 2017[1] , Elizabeth Denham was making it clear to companies in the UK that the upcoming changes from GDPR would represent a fundamental shift in their business. Denham, the UK Information Commissioner at the Information Commissioner’s Office (ICO) , was outlining how GDPR and the tailoring of the Data Protection Act 2018 would modernise the laws that protect the personal information of individuals.

Introduced on 25th May 2018, the General Data Protection Regulation (GDPR) marked a shift in the ICO’s powers to enforce the appropriate management of personal data. The regulation clearly expresses the rights of individuals, as well as the obligations placed on organisations.

Individuals would have easier access to information held about them by companies, as well as the right for this information to be removed; what became known as the ‘right to be forgotten’.

Companies would have requirements placed on them around the mandatory notification of data breaches to the ICO, whilst the regulator would have power to dispense well publicised fines and penalties which could reach as much as 4% of global turnover of the organisation in question. Even if fines were not imposed, the ICO retained rights to issue warnings and reprimands, to temporarily suspend data processing capabilities or demand the restoration or erasure of personal data.

Such a perceived seismic shift left many companies exposed due to their lack of appropriate preparedness, and the implementation date for GDPR loomed. This paper aims to assess the landscape now:

- What have we seen happen within the last 18 months
- What role have the ICO played, and how far have they exercised their power
- What have been the key impacts on organisations as a result of GDPR
- How organisations continue to mitigate the risk around data

We hope that you will find this white paper to be useful and would welcome any feedback.

Jonathan Harrison
Director

Henderson Insurance Brokers Ltd, an Aon company
Trueman House
Capitol Park
Leeds
LS27 0TS

T: +44 (0) 113 3936307
M: +44 (0) 7889 168032
jonathan.harrison@hibl.co.uk

www.hibl.co.uk

[1] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/01/information-commissioner-talks-gdpr-and-accountability-in-latest-speech/

18 Months of GDPR

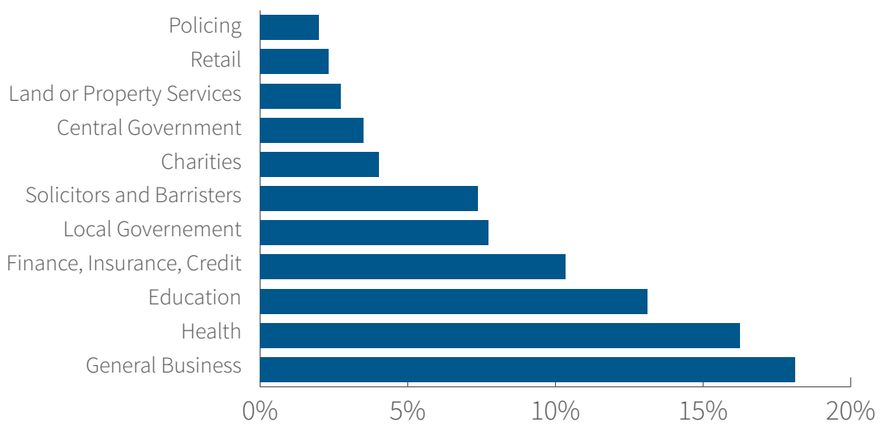
Reports post GDPR have been varied in the interpretation as to the extent that the ICO have exercised their heightened capabilities. In real terms, in the 2018/2019 period the ICO received notification of 13,840 personal data breaches:

Indeed, of these notified breaches only
- 0.39% had improvement actions required, and
- 0.05% were issued with civil monetary penalties

The key offending sectors were General Business, Health and Education, perhaps the latter two as little surprise given their reliance and management of vast amounts of personal data.

"In 82% of cases assessed, we have determined that the organisation had measures in place or was taking steps to address the breach without further action being required by the ICO[2]"

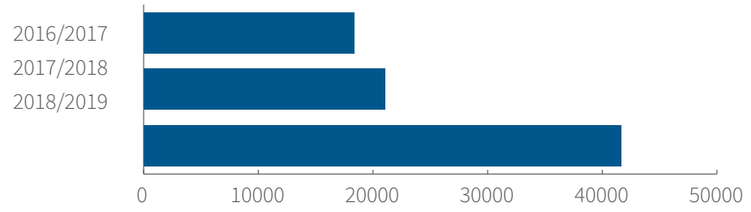
Sectors - Personal Data Breaches Reported 2018/2019[3]



[2] ICO Annual Report 2019/2019 - https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf, pages 28-29
[3] ICO Annual Report 2019/2019 - https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf, page 30

Where there has been marked increase is in the number of public complaints relating to data protection:

Data Protection Public Complaints - Annual[4]



38% of the complaints raised in relation to data protection in the 2018/2019 period were relating to SARs (Subject Access Request), with 16% raised for disclosure of data and right to prevent processing respectively[5]

Emma Roe, Partner at Shulmans LLP, suggests this increase in complaints should come as no surprise. The clear increase in general public awareness as to what data privacy means to them has given rise to what Roe terms as "empowered data subjects".

Roe also suggested the root cause of many data issues within companies was not as a result of cyber attacks, but rather the perceived lower risk of employees' own errors, omissions, or in parts disgruntled actions.

The ICO's Q4 statistics relating to non cyber personal data breach reports would support this:
- 2,577 non cyber personal data breach reports
- 536 of these were as a result of data being posted or faxed to the wrong recipient
- 392 were as a result of data being emailed to the wrong recipient

By contrast there were 686 cyber personal data breach reports in the same period, with 54% as a result of hacking or unauthorised access.

Roe raises a final point in relation to the ICO investigations that are launched as a result of the public complaints, in that companies are grossly underestimating the impact this has on their business; be that cost/productivity, the regulatory aspect from a legal standpoint, and in terms of general disruption to the business. The rise of the "empowered data subjects" could, without sound data risk management, cost the operation greatly.

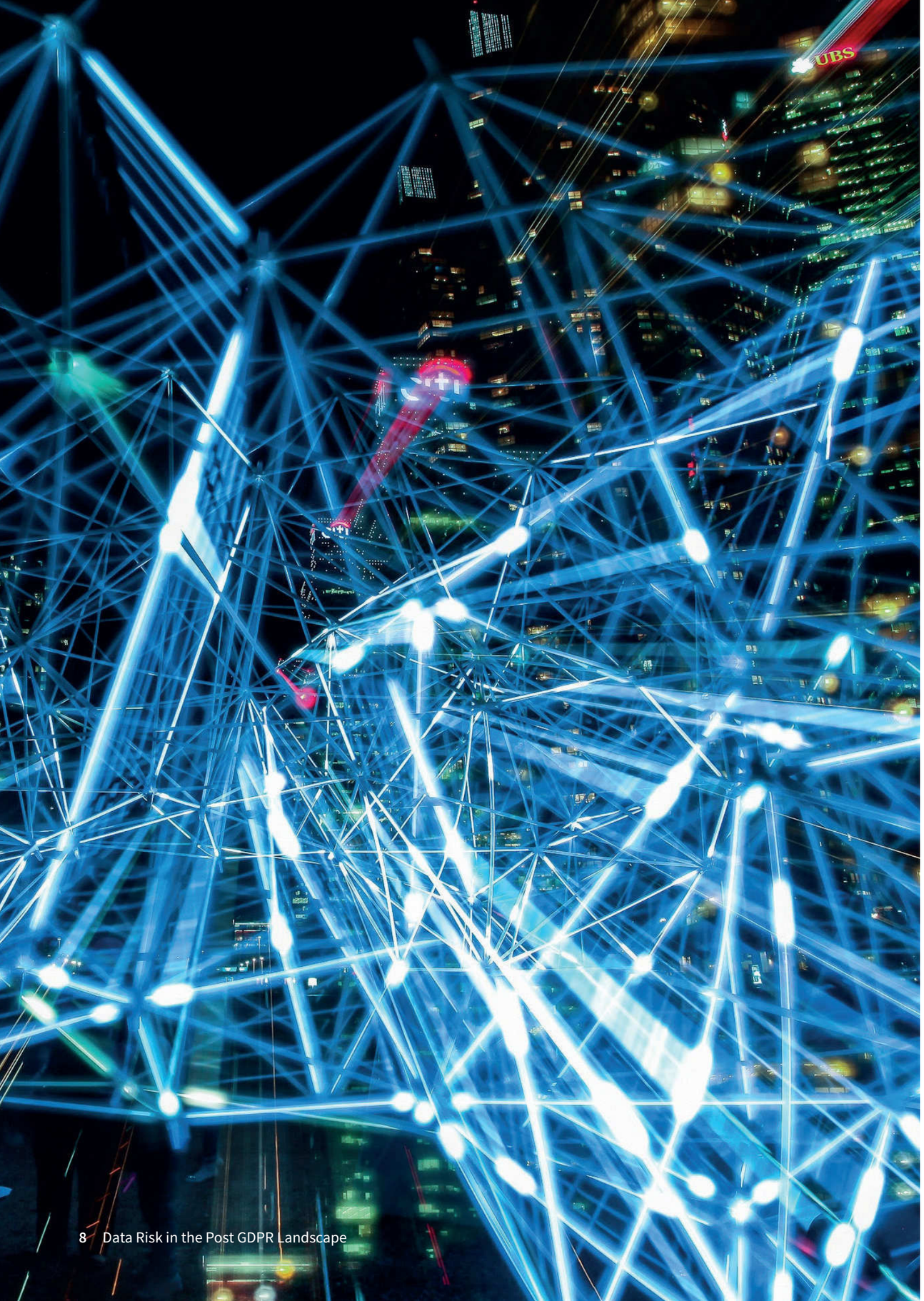
Whilst there is a continued focus on cyber security from hacking, denial of service attacks and the like, the statistics clearly highlight a need to develop a sound culture around data security awareness and process with employees at all levels of an organisation. This should form a key part of employee induction, ongoing training and awareness and continual improvement. How organisations manage the responsibility for data security throughout their structure should be embedded into their corporate governance procedures.

Vanessa Leemans, Chief Commercial Officer at Aon Cyber Solutions EMEA, suggests that:

"GDPR compliance can also strengthen customer relationships. Public opinion on data privacy is changing and customers are increasingly placing importance on how organisations protect their personal information. GDPR provides the chance to reinforce their role as responsible stewards of personal information and to craft innovative privacy and security policies that better reflect the constantly evolving needs of digitisation"[6]

Thus it is for organisations to continue to utilise GDPR as a potential positive springboard from which to invigorate their policy and procedure around data protection and security. Equally Leemans infers that companies that have a marked and noted commitment to GDPR compliance will ultimately breed closer brand loyalty over competitors.

[4] ICO Annual Report 2019/2019 - https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf, page 30
[5] ICO Annual Report 2019/2019 - https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf, page 31
[6] The price of data security - A guide to the insurability of GDPR fines across Europe, May 2018, AON/DLA Piper, https://www.aon.com/attachments/risk-services/Aon_DLA-Piper-GDPR-Fines-Guide_Final_May2018.pdf, page 4



ICO – Fines, Penalties and more

In the period 2018/2019 the ICO issued 22 fines which were as a result of legacy breaches of the Data Protection Act 1998 totally circa £3m[7]. A number of these fines were high profile and covered in the media, with the ICO putting cyber security at the centre of the causation:

"Cyber security is at the heart of some of the biggest personal data breaches that we have been investigating during the year. Three of the major fines….were as a result of failure in cyber security"[8]

This reinforces that the expectation on an organisation would be to have sound and tangible cyber security protections around all operating systems, and especially around the management of personal data.

In addition to this, the ICO have chosen recently to flex their GDPR muscle by implementing fines under the regulation:

- On 8th July 2019, British Airways were fined £183.3m following a hack which exposed personal data of 380,000 passengers
- On 9th July 2019, Marriott International were fined £99.2m for exposing the personal data of circa 330m customers worldwide

It is clear that the ICO are looking to set an example here, but interestingly fell short on both occasions of imposing the maximum fine of 4% of global turnover.

Alison Manley, Claims Relationship Manager at Travelers Europe, states that one of the issues with such high profile cases is that it may breed "levels of complacency" with SME organisations, in that they may seem out of reach of the ICO. This complacency should be disregarded, and SMEs continue to place data protection and security high on their board level agenda.

Regulatory actions taken by the ICO have a potential significant impact on any company from both a time and expense angle. Cyber Liability insurance policies widely afford regulatory defence costs, as well as affording support services and legal counsel from the notification process to the ICO, through the investigation, and to its conclusion. This facet to the Cyber Liability coverage is a key tool in the notification process.

Alison Manley also highlighted that there had been a "notable rise" post GDPR in policyholders raising queries around regulator notification and management of potential breach scenarios.

What remains unresolved is insurers' position in relation to the payment of ICO fines and penalties under a Cyber Liability policy. Under some wordings there is no coverage for any fines and penalties whatsoever, but under others only criminal fines are excluded and fines are included within the scope of coverage to the extent that they are 'insurable by law'.

Aon and DLA Piper suggest in their overview of the insurability of GDPR fines that:

> *"GDPR fines are not expected to be insurable in the UK. Although there are rare case law exceptions to the public policy rule against indemnity, they are not expected to apply to the administrative and criminal fines that will be imposed under proposed legislation."*[9]

The issue for many companies is the unanswered, or put better perhaps untested, scenario in relation to fines and penalties. However, it would remiss not to consider this a further reason to retain Cyber Liability coverage and await case law examples in due course.

[7] ICO Annual Report 2019/2019 - https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf, page 9
[8] ICO Annual Report 2019/2019 - https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf, page 35
[9] The price of data security - A guide to the insurability of GDPR fines across Europe, May 2018, AON/DLA Piper, https://www.aon.com/attachments/risk-services/Aon_DLA-Piper-GDPR-Fines-Guide_Final_May2018.pdf, page 19

Company Impact

It is evident that occurrences of data breaches are on the rise. According to Carbon Black's second UK Threat Report, 88% of UK organisations reported suffering a breach during the last 12 months, with the average number of breaches per organisation over the past year reaching 3.67[10]. But on what levels more specifically does this impact upon a company?

Reputational damage following regulatory action

We have touched briefly on the potential significant costs that a regulatory investigation could bring to an organisation. But a data breach brings with it other key considerations:

- Notification to the ICO following a breach should be within 72 hours; this entails significant manpower and engagement with various third parties in a finite amount of time
- The ICO can impose mandatory notification to other data subjects, and dependent on data records held these costs could be substantial
- Credit monitoring costs could also be imposed
- Reputational risk and damage, and resultant Business Interruption

It is clear from the media coverage on a number of the high-profile data breaches in 2019, British Airways for example, that there is immediate brand and reputational damage following a data breach. This is an area where insurers are making a clear advocacy for Cyber Liability policies, the majority partnering with specialist Public Relations consultants to support and guide policyholders through a data breach, to minimise brand and reputational damage, and minimise business interruption.

In real terms, data breaches can significantly affect the value of your business. Yahoo!, for example, had to lower its asking price by $350m for its acquisition by Verizon after it suffered a huge breach that affected millions[11].

Or consider the well-publicised data breach by TalkTalk, who were crippled with incoming enquiries from existing customers around the loss of data. To quantify this, it is estimated they lost circa 100,000 customers[12]. There has been significant discussion around the CEO's dealing with the media post breach, and undoubtedly a stronger PR line and strategy to minimise reputational damage would have been invaluable here.

Impact of remote working

As remote working continues to become an embedded part of organisational culture, the data security risks have also increased exponentially. It is expected that 50% of the UK workforce will work remotely by 2020[13].

Research from CybSafe suggests that a third of UK businesses have suffered a data breach because of remote working in the last 12 months[14].

However, remote working relies on two things:

- Putting security practices and policies around employees and their systems to minimise the likelihood of a breach, including basic security precautions and the like
- The understanding that employees will follow such procedures, not deviate and potentially jeopardise data security

On the latter point, CybSafe suggest that most decision makers are "over-confident" when it comes to remote working. It is suggested that only 50% have provided adequate training to their staff in the last 12 months[15].

One such area where employees can commonly fall foul is the use of personal email addresses – according to ProBrand nearly two thirds of UK employees have forwarded customer emails to their personal email accounts, and 84% of them did not feel they had made an error of judgement[16].

Therefore it is imperative that to support the remote working trajectory, that proper cyber security measures are implemented and organisations effectively train their employees (whether working remotely or office based) on data risk management.

More human error – social engineering

This type of attack is in which criminals fraudulently impersonate a legitimate person or organisation. One of their methods of attack could well be to trick employees into handing over sensitive data, but more often than not this could also be downloading a malicious attachment or providing access to their organisation's system.

Phishing is the usual method through which employees would be misled into disclosing such information.

Again, the costs could be significant for an organisation, and some Social Engineering losses (especially with fraudulent funds transfer) bridge both Cyber Liability and Crime insurance coverage. The lack of understanding of the nuances between the two in the broking community often leads to companies being left exposed, whilst assuming coverage is in place for all such eventualities.

The real cost of a data breach

Following the publication of its fourth annual breaches survey, the Department for Digital, Culture, Media and Sport (DCMS) has noted that costs of data breaches to companies are rising. The average cost of a business breach in the UK (with data ranging from micro to major businesses) in 2019 is £4,180. This has increased from £2,450 in 2017[17].

It is worth highlighting that associated losses such as brand/reputation and ongoing business costs are not included within this figure, but instead this is the quantified cost of the data breach loss. If we take the assumption that on average companies are having, on average, 3.67 breaches annually then these real costs are set at £15,340, and this is without considering additional losses from business interruption and reputational damage.

[10] https://www.techradar.com/uk/news/88-of-uk-businesses-have-been-breached-in-2018
[11] https://www.techradar.com/uk/news/the-true-cost-of-a-data-breach
[12] https://www.techradar.com/uk/news/the-true-cost-of-a-data-breach
[13] https://www.techradar.com/uk/news/the-dark-side-of-sending-work-emails-home
[14] https://www.techradar.com/uk/news/remote-working-is-leading-to-a-rise-in-data-breaches
[15] https://www.techradar.com/uk/news/remote-working-is-leading-to-a-rise-in-data-breaches
[16] https://www.techradar.com/uk/news/the-dark-side-of-sending-work-emails-home
[17] https://www.securityweek.com/cost-data-breach-uk-increases-more-41-two-years

Mapping the GDPR Landscape – Mitigating Risk

It is hard to escape the fact that many view GDPR as a 'Millennium Bug' regulation; something that came and went and has had little impact in terms of the day to day operation of many organisations. The truth, however, is that the regulation has had far reaching effects:

- It has led to data subjects becoming increasingly aware of their rights in relation to data privacy and security
- It has made many companies turn the mirror on their operational standards in data risk management and change for the better
- It has led the to the ICO taking action and looking to set a new standard in appropriate data management within companies

What is less clear is what the future landscape looks like. Data breaches, both significant and more modest, will continue to happen. It is the level of preparedness that companies have in place that will ultimately determine as to whether the effects can be absorbed, or if it causes damage to their brand and reputation beyond recognition. The Cambridge Analytica saga only goes to prove how seismic poor data management can be, and how likely fervent public reaction is.

Organisations with a clear commitment to responsible data risk management will stand shoulders above their peers through:

- Sound implementation of privacy and data management procedures throughout their organisation
- The removal of complacency around employee contact with data – there should never be the assumption that the employee will always do the right thing
- Challenging emerging risks such as remote working face on, and ensuring that training for all employees is a key risk management agenda item
- Proper and proactive cyber security systems, which are regularly updated
- Legal advice on good, realistic GDPR management, and also on how to deal with a data breach should it happen
- A real consideration to include Cyber Liability within and risk and insurance programme as a transfer mechanism for some of the exposures that GDPR bring about

As the landscape continues to shift, it is evident that the broking community also have an ongoing responsibility to educate organisations on the availability of coverage, and the specifics on issues such as coverage for fines and penalties. Insurers it seems will continue to be challenged on breadth of wording, and on potential cross-policy issues such as Social Engineering bridging Cyber Liability and Crime policies.


APC
GRIDSTORE
Violin
NUTANIX
KARMA

This paper was written as part of the Travelers Techsure Academy 2019. Techsure Academy provides a unique training experience for insurance brokers wishing to develop and refine their tech knowledge and who are looking to increasingly specialise in this exciting and evolving sector. For more information, visit travelers.co.uk/techsureacademy