Statement from Sara Duncan, director of Crew and Concierge Limited, to Verdict:

I founded my company, Crew & Concierge, over 13 years ago and I have worked hard to build a strong reputation for providing competent and reliable crew to work on the private yachts of the most incredible clients. I employ three people, we are a very small bespoke business.

As a small business owner, it has been extremely hard work and I believe that the reputation we have built for Crew & Concierge is largely due to sheer determination to ensure we provide the best service possible to meet the requirements of our valued clients and crew.

Confidentiality, privacy and security have always been of paramount importance for the success of the company. I realised this right from the start. These three pillars of our business underpin everything we do and inform all our commercial decisions.

So, in early 2018, when it became clear that our business would soon outgrow our IT systems, we went out into the market for a highly scalable and robust IT strategy. We also selected a team of developers based on their expertise and experience to build a system that would deliver the resilience and security needed for our growing business and give us the best usability and the highest protection for the large volumes of data we handle. We selected Amazon Web Services, based on the confidence we had in their security record and the reputation as one of the world's leading cloud service providers. The guarantees on resilience, availability and security were – and remain – the main reasons for our informed decision, while the increased functionality was clearly a bonus.

From the moment we learnt of the breach my team and I have worked tirelessly to identify the sources of disclosure, detect the areas of weakness, close the vulnerability, recover control of the data, identify precisely what data was compromised, and minimise the potential risk and harm to the affected individuals.

Within two hours of you contacting us to notify us of the breach, we had:

- ***Identified the cause****
- ***Locked down the entire S3 file store to block all public access;***
- ***Successfully tested to ensure that it was no longer possible to access any files from outside the application;***
- ***Contacted the hacker to request that he take down and destroy all copies of the data he had exfiltrated, and received his confirmation that he had done so;***
- ***Confirmed with you that you were no longer able to access the file store to which you previously had access.***

**** To allow the files to be transferred from the previous developers to our new S3 store, an Amazon bucket was created to store the files whilst they were being migrated into the new application. This bucket was open only to an authenticated***

AWS user, in order to allow the previous developers to connect to and transfer the files. The reason the archive file store wasn't deleted immediately was so that we could safeguard the data transfer and reduce the time to go back and correct any errors, although we deemed that the likelihood of this risk to customer data vs losing customer availability was a sensible decision.

Within 24 hours, we had:

- ***notified the Information Commissioner's Office and sought their guidance;***
- ***reported the matter to the police, National Crime Agency and to ActionFraud;***
- ***instructed a solicitor with specific experience in data breach response;***
- ***engaged Simon Hall of AwarePrivacy, a leading privacy specialist; and***
- ***engaged Sean Atkinson of Secarma, a security specialist with extensive experience in AWS configuration, vulnerability exploitation and remediation.***

Since notification, we have issued three updates to the ICO and will continue to issue updates as further information comes to light.

Of the 90,000 files that you told me had been compromised, we have identified the most sensitive documents and the affected individuals and are in the process of mapping individuals to other types of document and personal information that were compromised.

We have now successfully risk rated each individual and are following ICO guidance on notification requirements and remediation.

Notifications will be transparent and responsible, offering such assistance and support as may be necessary to ensure a fair and proportionate response to the risk in each case, all in line with ICO guidance and the advice they are giving us.

We can confirm that 1295 scanned copies of passports were compromised of which we can tell you 272 passports have expired. 42 of those Passports are still being reviewed due to a complication with this data.

We also believe that 1419 ENG1 forms were compromised – we have reviewed them individually to identify the level of sensitivity of information in each case and again 655 of these have expired. 294 of those ENG1's are under further investigation.

In total, personal information relating to 17,379 crew members has been compromised. In approximately 15,000 cases, the information was limited to CVs with or without supporting certificates evidencing professional qualifications and competencies.

So a large proportion of the 90,000 documents compromised in this breach contained very limited personal information or none at all – documents such as themed menus and *crew food plans; details of experience in engineering and carpentry; Food & Hygiene certificates; attendance records for Fire Fighting, First Aid and Personal Safety at Sea courses; and certificates for qualifications in hairdressing, beauty, wine, personal training and yoga.*

Back to the technical side, we have been advised by the cyber-security consultant that exploitation of s3 buckets is by no means a straightforward activity and that it

appears likely that the individual or individuals responsible have developed advanced tools designed specifically to identify AWS customers and whether or not they have misconfigured instance that may leave it open to malicious attack.

In our case, the confidence was placed in the team of developers we had hired, trusting that they would do a competent job and implement appropriate and proportionate technical and organisational measures to ensure the protection of the large volumes of information, including personal and sensitive personal information relating to our registered crew.

We have since established that the breached AWS S3 bucket that we outsourced contained personal data stolen by a malicious actor/s based on a misconfiguration by a third party and published into the public domain.

This impacts Crew and Concierge, and its valued clients and staff, for which we take full responsibility as the data controller. In the very short period, we have come to understand the true impact of a Cyber Attack, and we have learnt many valuable but hard lessons.

I would like to confirm that to date we have no confirmation from the journalist or the site that exposed our data that these files have been accessed.

An independent Cyber Security Expert has said:

"This is a very interesting case, based on a number of factors.

1. ***I work with companies who 'should' report, respond and react in the way Crew and Concierge have done over the last 4 days, who are all much larger, more mature and should see this as a pretty good Cyber Incident Response.***
2. ***Sara is a businesswoman, not an IT specialist and certainly not an InfoSec expert. Nor do they have the budget, resource, or maturity to ever realistically believe they would be the target of a breach. No excuse, but the way they have sought experts, cared about their clients and what to do next, put preventative measures in place, planned and reported has been exemplary.***
3. ***I don't suspect it is a targeted, at all, but it does show that cyber-attacks can and will happen to anyone.***
4. ***For me, the 'broker' in all this needs more attention than Crew and Concierge.***
5. ***Championing Cyber Security is a big passion of mine, but the above is a better story for me."***