Insurance Times



# Hasty migration could increase corporate cyber risk exposure

By Clare Ruel | 21 May 2020

**With another high-profile cyber attack case during lockdown, a new challenge has been created for brokers**

As businesses continue to work from home during the Covid-19 pandemic, the spate of cyber attacks has increased but brokers should continue engaging with security analytics services to support clients, *Insurance Times* has heard.

Most recently, British low-cost airline easyJet fell prey to hackers and as a result could face a hefty fine. The airline suffered a cyber-attack affecting 9 million customers with the credit card details of 2,208 potentially compromised.

Erin Kenneally, director of Cyber Risk Analytics, at Guidewire Software told *Insurance Times*: "The most obvious value is that malicious actors can use travel details (in this case, name, email address, origin and destination, departure date, booking reference number and transaction amount) to create

more tailored, personalised spear phishing attacks to lure consumer-victims into exposing more sensitive and value-laden data for fraudulent purposes."

When asked how brokers can support clients, she said: "Until we know more about the attack vectors it's hard to assess if and to what extent easyJet could have prevented this incident, but in general as carriers and brokers continue to become more involved in risk management, they should engage security analytics services like Cyence that provide predictive risk signals to increase the value proposition for risk prevention in addition to traditional indemnity."

## On comparison

Speaking about whether easyJet could face a fine similar to that of British Airways (BA), Kenneally added: "Based on preliminary information is does not seem likely that the fine would be on the order of the $224m issued to BA." This she said is due to a number of reasons:

- The BA hack posed a much higher risk, both qualitatively and quantitatively- it exposed about a half a million records which included payment card details such as CVV and billing addresses versus 2,208 sensitive credit card information for easyJet and the rest being travel metadata.
- If in fact this was a sophisticated hack the ICO (Information Comissioner's Office) may be more lenient, as the BA incident was owing to a well-known vulnerability in third-party javascript on its website which had not been updated since 2012, so it was a known-known
- There may be an element of real politicking, since the BA incident occurred a short while after the implementation of GDPR in May 2018 and data protection officials may have been keen to set an example and demonstrate their commitment to enforcement.

## Value of personal data

Adrian Nish, head of threat intelligence at BAE Systems Applied Intelligence, told *Insurance Times*: "This case is another reminder of the value of personal information to criminals and hostile state actors.

"The focus now is on airlines, but previously we've seen telecoms firms and hospitality industry targeted. Insurance has also been in the cross hairs in previous years, with firms in North America, as well as Europe attacked for their sensitive information."

Sources reported by *Reuters* said that the group of hackers had previously targeted travel records and other data in a bid to track specific movement of individuals.

"Interest in who is travelling on which routes can be valuable for counter-intelligence or other tracking of persons of interest," said Sahar Naumaan, threat intelligence analyst at BAE Systems who has investigated similar attacks.

## Expanded exposure


EasyJet hit by major cyber attack affecting 9 million customers

Meanwhile back in April near the start of lockdown, the Marriott being attacked for a second time illustrates that is sensible for businesses to manage risk effectively.

Tim Smith, partner at law firm BLM told *Insurance Times:* "It is still wise for businesses to do everything they can to manage their risk – be that technical, physical or human, whether that be by using the latest technology and software, using robust passwords, using two-factor authentication, using encryption, making sure premises and documents are keep secure and providing training."

At the time of the Marriott attack, Kenneally said: "As Covid-19 has spread across the globe, so corporate cyber risk exposure has expanded. As businesses adopt remote working, a resulting consequence is an increase in the number of potential targets available for exploitation by cyber criminals.

"Business susceptibility to cyber risk during the Covid-19 pandemic can result from the hasty or ill-prepared migration of the workforce to remote operations, where employees access internal corporate networks from outside the core corporate infrastructure."

Keneally warned that insurers must consider how the lack of a standardised approach to remote operations may impact the level of risk.

"This remote work approach should include defined standards, guidelines, best practices, tools, and collateral that address the risk and challenges of remote work in areas such as remote team enablement, collaboration tooling, security, project governance, management of different environments, working across multiple time zones and workshop facilitation," she added.

## Not sufficient enough

Speaking of the data that had been stolen in the easyJet attack, Austin Berglas, global head of professional services at cybersecurity firm BlueVoyant said that although this was not sufficient enough to commit identity theft or financial fraud on its own, the theft of emails and travel plans could be used to launch phishing campaigns against the affected individuals.

“Combined with other personal information scraped from public social media profiles, these stolen emails can be customised and crafted to target the individual, thereby increasing the likelihood that the victim will be induced to provide passwords or sensitive account access, Berglas said.

“In addition, sensitive accounts might be at risk as email account passwords can be obtained in the dark web and many users reuse passwords across multiple accounts.

”The use of multi factor authentication and practising proper password hygiene is a necessary step to best avoid account takeovers which may lead to identity theft or financial fraud - in addition, putting in place a credit freeze will also greatly reduce the chances of identity theft.”

## Known and preventable

But on a more positive note, Kenneally said that the threats businesses are dealing with are largely known, preventable and can be defended.

“Considering the risk factors related to remote working, threats such as spear phishing, social engineering, spam, and denial-of-service attacks have already intensified and are expected to continue along that trajectory.

“Central to reducing cyber exposure is understanding the nature, scope, and projected impact of the cyber risk.

”This is critical for insurers to define segments and tailor pricing, determine bad risks, understand the risk exposure across their portfolio, and determine the degree of claims automation,” she told *Insurance Times*.

---

**Read more...How GDPR changed the world and the way it handled data**

***Not subscribed? Become a subscriber and access our premium content***