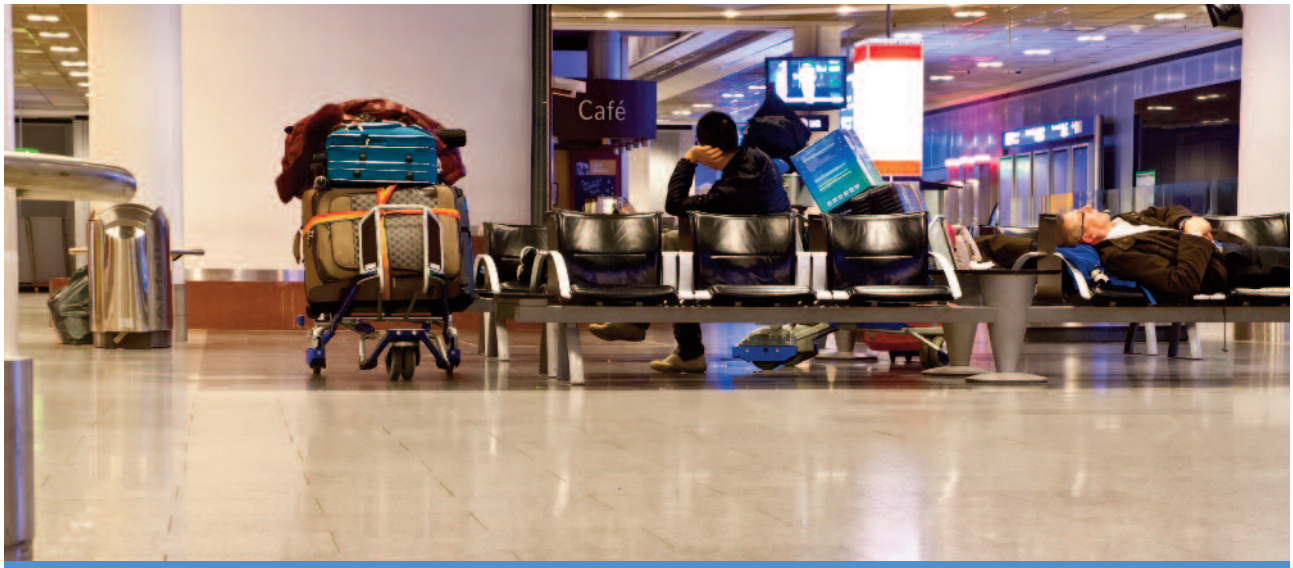
CYBER DECODER

FINANCIAL LINES GROUP NEWSLETTER ISSUE 5



OFFICE OF PERSONNEL MANAGEMENT UNDER THE SPOTLIGHT
Page 2

TOP TWEETS
Page 2

SONY'S EMPLOYEE LAWSUIT MOVES FORWARD
Page 3

AUSSIE TELECOM COMPANIES TO FACE FINES OVER CYBER SECRURITY
Page 4

Aviation cyber risks

Investigations are still ongoing into the suspected hack that resulted in several grounded planes and 1,400 more-than-disgruntled passengers at one of Poland's busiest airports.

The outage, which lasted five hours, saw twelve flights to various European destinations delayed and ten flights cancelled altogether. The carrier reported that despite the action down on the ground (or the lack of it) airborne aeroplanes were in no danger.

This case is by no means the first aviation cyber incident we have seen in the press. At the end of 2014, Japan Airlines reported it had been breached by an external malicious. As many as 750,000 customers, the majority of whom were on the airline's loyalty programme, had sensitive information compromised including names, date of births and email addresses. In 2015, a cybersecurity consultant claimed to have hacked into aircraft whilst they were flying, through the on-board entertainment systems, on at least 15 different occassions. Additionally, he maintained that on one occasion he was able to adjust the plane's course of direction and force it into a climb. It is critical for risk managers to assess the cyber exposures their company might face, particularly at a time when airlines seem to be an increasingly frequent target. They would find value in sitting down with their insurance broker to run through loss scenarios. A good starting point would be the three scenarios mentioned above! Do your current policies cover these? Stress test your traditional policies, identify the gaps and see whether a robust cyber policy is an option. ■

Office of Personnel Management under the spotlight

In what is being described as one of the worst breaches to date, the federal Office of Personnel Management (OPM); the US government's human resources division, reported it had suffered a breach that exposed four million employees personal information. The hackers, believed to be Chinese, stole a wealth of personally identifiable information, inckuding current and former employees' financial information, dates of birth and security numbers. The worry is that information on workers' friends and family as well as their personal employment, criminal and medical histories, was also taken, giving rise to the fear of blackmail.

Although reports are conflicting, the general consensus is that it took four months for investigators to discover the breach allowing the infiltrators enough time to delve deeper into the company's databse. Some reports suggest that members in the military and intelligence agencies also had their details exposed, putting them at serious risk.

Where did it all go wrong? OPM was heavily criticised for the lack of measures it took to protect the sensitive information it held. In a grilling from members of the House Committee on Oversight, OPM admitted that it had been warned by the inspector general that its IT security had been poor since 2007. The lack of encryption was highlighted as one of the fundamental flaws in the OPM breach, making it much easier for the hackers to gain access. Claims analysis identifies encryption as being an effective tool in cybersecurity. When buying a cyber insurance policy, underwriters will look to see whether your company encrypts its data. As the process of deploying encryption has become less onerous than in the past, it's tougher than ever to explain if you haven't considered it. ■

TOP TWEETS

Our @JLTGroup CEO Dominic Burke talks about the growth of #cyber insurance http://buff.ly/1CngSXU

New data protection regulation must not reduce level of protection, says EU privacy watchdog http://buff.ly/1HAYKWi

90% of firms have been subject to a cyber breach in the last year http://buff.ly/1G2AYmn

Asset managers at risk from cyber-attacks http://buff.ly/1R8RczC

Health warning: Now e-cigarettes can give you malware http://buff.ly/1LKWvqC

FCC Settles First Data Security Action http://buff.ly/1I2t40A

Directors - what are your cyber-security responsibilities? http://buff.ly/1MpaoYN

@JLTGroup reveal the biggest cyber trends in a video interview with StrategicRISK: http://bit.ly/1GKljr6 @sarahmstep

43% of mid-sized businesses have suffered this loss, but only 20% have coverage http://buff.ly/1GWVKX6

Sony's employee lawsuit moves forward

On 24th November 2014, Sony Pictures Entertainment employees made their way to work on a crisp Monday morning and settled down to their jobs. Switching their monitors on they were immediately greeted by a leering face and the proud proclamation 'Hacked by #GOP'.

We later discovered Sony's studios in Culver City, California, had been hacked by what some reports believed to be North Korea on account of the film 'The Interview' which dramatized the assassination of their leader Kim Jong-un. Sony suffered on several accounts including business interruption, loss of sensitive data and exposed intellectual property.

> 47,000 social security numbers, medical and salary records were exposed.

The all-too-familiar pattern in the US of the litigious warfare that rages between employee and/or customer and breached company may very well occur in Europe with the upcoming EU Data Regulations playing a big role in breach notification. Those individuals who believe they were affected by the breach argue the company could have done more to protect their credentials; the company furiously defends itself claiming it had done everything to protect the data held. In Sony's case, the plaintiffs described the exposure as an 'epic nightmare' believing the company had failed to improve their security systems despite having known they had weaknesses for ten years. 47,000 social security numbers as well as medical and salary records were exposed.

Earlier this month it was ruled that Sony was unable to dismiss the lawsuit brought against them by nine former employees. The judge granted the plaintiffs permission to pursue claims that Sony had been negligent in the storing of their personally identifiable information. He further stated that there were grounds for suing Sony as they had violated various Californian confidentiality laws, stating they could have done more to protect their former employees' health and salary data. Sony's CEO claimed previously that their cyber insurance was fully covering the costs from the incident, so we'll be closely watching to see if any coverage issues – including limit exhaustion crop up for Sony. ■

JLT Specialty Limited provides insurance broking, risk management and claims consulting services to large and international companies. Our success comes from focusing on sectors where we know we can make the greatest difference – using insight, intelligence and imagination to provide expert advice and robust – often unique – solutions. We build partner teams to work side-by-side with you, our network and the market to deliver responses which are carefully considered from all angles.

Our Cyber, Technology, and Media Errors & Omissions team delivers bespoke risk management and insurance solutions to meet the needs of clients from a variety of industries. The team combines experience and talent with a track record of delivering successful results and tangible value for our clients.

CONTACTS

Sarah Stephens
Head of Cyber, Technology and Media E&O
JLT Specialty
+44 (0) 20 7558 3548
sarah_stephens@jltgroup.com

Lauren Cisco
Partner, Cyber, Technology and Media E&O
JLT Specialty
+44 (0) 20 7558 3519
lauren_cisco@jltgroup.com

Jack Lyons
Partner, Cyber, Technology and Media E&O
JLT Specialty
+44 (0) 20 7528 4114
Jack_lyons@jltgroup.com

JLT Specialty Limited
The St Botolph Building
138 Houndsditch
London EC3A 7AW
www.jltspecialty.com

Lloyd's Broker. Authorised and regulated by the Financial Conduct Authority. A member of the Jardine Lloyd Thompson Group. Registered Office: The St Botolph Building, 138 Houndsditch, London EC3A 7AW. Registered in England No. 01536540.
VAT No. 244 2321 96.

BUZZWORD OF THE MONTH

TAKING THE BUZZ OUT ONE WORD AT A TIME

RANSOMWARE

What it means:

Ransomware is a malicious file which is designed to extort money from a user by disabling their computer or encrypting files stored on the computer. The user is then informed that they must pay a ransom to have the files restored. The ransom prices vary, ranging from USD 24 to USD 5000, or bitcoin digital currency equivalent. Ransomware infiltrates a computer after a user clicks on a link or attachment in an email or when a user visits a website, including well-known sites with good security systems.

Why you should care:

If ransomware encrypts all the files on your computer you will have the option to pay the cost. If you decide to pay, the hackers may send users a computer code to unlock the files one by one, so depending on the number of files, the process could take weeks. However, it is important to note that there is a risk that after paying the ransom, the user will not regain control of their system.

According to the McAfee Labs Threats Report in May 2015, ransomware attacks surged 165% in the first quarter, and this trend is likely to continue as this type of cyber attack can be extremely profitable for the hacker. In 2013, the US Department of Justice estimates that a group of hackers made USD27million using ransomware in just two months. Many cyber insurance policies offer an extension for cyber extortion, but make sure that you understand all the conditions, which may include specific notice provisions and confidentiality obligations. It's also a good idea to stress test your policy with a ransomware off-the-shelf situation to ensure that none of the off the shelf terms should be modified to assure coverage.

Aussie telecom companies to face fines over cyber security

Its crunch time for telecommunications companies in Australia as they could face fines of up to AUD 250,000 if they do not take necessary steps to protect government agencies and businesses from the threat of cyber attack. The regulations, which are potentially due this year, will ensure the safety of data for business, individuals and the public sector. The bill is still being passed through local government, so watch this space…..■