CYBER DECODER

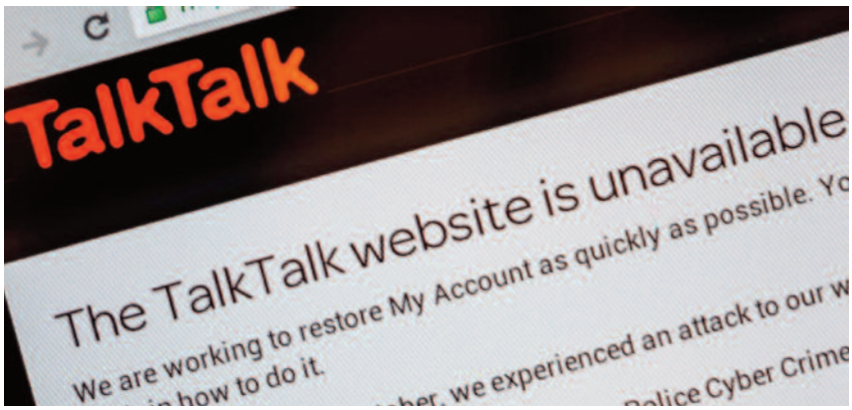
FINANCIAL LINES GROUP NEWSLETTER ISSUE 7

TalkTalk cyber attack

TalkTalk, a major UK provider of television, internet, and phone services, has been the victim of a cyber attack that was initially thought to have compromised the personal details of up to 4 million individuals.

The attack on TalkTalk, coming just months after the data breach at Carphone Warehouse, highlights the pervasive nature of cyber attacks on UK companies, as well as the often drastic steps that those companies are forced to take in a data breach situation. The fact that not all data held by TalkTalk was encrypted adds further troubles to the company that will inevitably have several additional expenses to follow. They are in the process of notifying the 4 million individuals affected and are offering a year of credit monitoring services to those individuals, which will carry a significant cost. It is important for companies not to panic at this stage and to consult their incident response teams immediately. They will be able to diagnose the breach and ascertain who exactly has been affected. This will help companies save time and money. Traditional insurance products aren't likely to respond to the potentially significant incident response costs, but if TalkTalk took out cyber insurance they would be receiving incident response support from their insurer amongst other services. It's important for companies to remember that security and insurance spending are not mutually exclusive. Neither are a complete solution that removes all risk, however combined will drastically help a company deal with threats it faces on a daily basis.

Continued on page 2 ▶▶



"If TalkTalk took out cyber insurance they would be receiving incident response support from their insurer amongst other services."

ADDITIONAL CONSIDERATIONS

- As with most high profile breaches, there have been consequential attempts to defraud the already affected consumers (criminal groups seizing on the opportunity to contact them in connection with the breach or using stolen information). It's unlikely that TalkTalk can be held directly liable for such losses, however that will not stop it from tarnishing their reputation or stop lawsuits from being filed.
- The UK Information Commissioner is already investigating them hence they are incurring investigation costs, and it's very possible that a fine will follow at some stage.
- TalkTalk has an almost GBP 300 early cancellation fee. This currently is still being enforced, so there will be a loss of revenue if they are either forced to or voluntarily stop this fee. As their business model is all about being lean and low cost, this event is likely to significantly impact their profits.

This incident, like the Carphone Warehouse incident before it and so many UK cyber incidents, should be a wakeup call for all UK businesses to take a serious look at cyber risk mitigation and insurance. ■

Cyber insurance market in its teenage years

At this year's Professional Liability Underwriting Society (PLUS) Conference in Chicago, Sarah Stephens partook in a series of debates which can be viewed on the PLUS website.

In one of the questions on whether the market for cyber insurance was sustainable or not, Sarah compared the cyber market to a teenager, believing it to be in its adolescent years. She explains her statement in more detail….

"We are at a point in the market where cyber has been around for roughly 15 years and because we don't have the amount of data that other lines of insurance have, cyber insurance does not have the 'life experience' to price the risk in the same way that property and casualty markets do. We are in the adolescent stage of the market cycle which is normal for the development of a new product. What will keep us on track to reach 'adulthood' is to continue due diligence around building robust and statistically significant modelling capabilities. It is important also to think about how brokers and insurers can drive more uptake because at the end of the day it's a numbers game – we need more cyber insurance buyers in order to withstand larger losses. Partnering with external technology and security firms is also important. Dynamic pricing models or constant monitoring should also be used to allow insurers to manage their books on more of a real time basis. These steps could help cyber insurance progress and grow." ■

To view rest of the interview click here

2016 – the year that EU data regulation finally bites?

The reform of data protection rules across the European Union (EU) has been a priority for the European Commission (EC) for many years.

The EC are concerned about the 'internet of things' and the impact it, and the globalisation of data exchange will have on civil liberties and the role companies and other bodies play in protecting it.

The European Data Protection Regulation (EDPR) will respond to these challenges by giving citizens control over their personal data and creating a clearer regulatory framework for businesses to operate within. At its core, the EDPR aims to upgrade and harmonise the current data protection laws in place across EU member states, by balancing the movement and processing of data with safeguarding individual privacy.

The EDPR will be a 'regulation' (as opposed to a directive) which will make it directly applicable to all EU member states without a need for national implementation of the legislation. Once the regulation is passed, it will replace the current assortment of national laws with a single set of rules. It will change the regime in the UK and the consequences associated with a data breach.

The EC are concerned about the 'internet of things' and the impact globalisation of data exchange will have on civil liberties, and the role companies and other bodies play in protecting it.

WHERE ARE WE NOW?

On 15 June 2015 the European Council agreed a common position on the EDPR and the key provisions are discussed below. While negotiations continue between the European Parliament, the Council and the EC, the aim is to reach a final agreement by the end of 2015. That said, the suggested deadline is unlikely to include the entirety of the EDPR and we will have a clearer picture of the timetable early in the year, once the next trilogue negotiations are to be concluded. It is unlikely that the EDPR will be enacted before autumn 2016.

WHAT ARE THE KEY PROVISIONS?

Territorial Scope

The EDPR will have a broad scope, applying to the processing of personal data by a controller or a processor in the EU and the processing of personal data of data subjects residing in the EU by a controller not established in the EU, where the processing activities are related to either the offering of goods or services to data subjects in the EU, or the monitoring of their behaviour as far as it takes place in the EU.

Continued on page 4 ▶▶

A 'one-stop shop'

The EDPR has created the role of a Lead DPA (Data Protection Authority e.g. the ICO in the UK) to be applicable in the country where the data controller or processor has its main establishment, or where the data subjects affected are located. The Lead DPA will have a duty to cooperate with any other DPAs concerned (e.g. the DPA of a country where a concerned party is domiciled) and work with them to agree on a decision.

Data breach and security

Data controllers and processors will have an obligation to implement appropriate technical and organisational measures to safeguard personal data from security risks. In the event of a data breach, data controllers will be required to notify the competent DPA within 72 hours and notify data subjects without undue delay.

The EDPR has also introduced the role of a 'Data Protection Officer' which it has left to the discretion of member states to adopt on a mandatory basis. The role would involve notifying data breaches to supervisory authorities and any individuals concerned.

ENFORCEMENT AND FINES

Entities that violate provisions of the EDPR could face fines up to EUR 1 million, or up to 2% of the global annual turnover of a company subject to the severity of the breach, taking into account the actions of a data controller or processor to mitigate the damage caused to individuals.

The 'right to be forgotten'

The EDPR, unlike the current regulations, will provide the right to be forgotten. Individuals will be able to ask data controllers and, in some circumstances, information society services to erase their data without undue delay, provided it meets the criteria required.

WHAT DOES THIS MEAN FOR THE MARKET?

Cyber insurance has been anticipated to be the next 'big thing' in the market for years but the take up has been slower than anticipated across the UK and the EU. This is set to change as the EDPR will burden companies to ensure they have appropriate security procedures in place to prevent the loss of data and appropriate mechanisms to ensure that any data breaches are notified within a tight time-frame. Insurers are increasingly aware of the implications of the EDPR and its implications are ranking highly on companies' risk registers. As a result, there are more underwriting teams dedicated to writing such business.

The structure and presentation of such cover is a keen consideration for insurers, particularly as it is difficult for companies to quantify potential loss of profits resulting from a data breach. However, a data breach is only one aspect, loss of profits resulting from cyber-hacks include a variety of intangible assets, such as the brand and corporate reputation or intellectual property. The EDPR heightens the uncertainty concerning loss of profits as companies could face unpredictable notification costs by complying with the 72 hours' time-frame, and increased regulatory fines of 1 million Euros or 2% of their global turnover in comparison to the current maximum fine of GBP 500,000 in the UK.

In response, there is likely to be an increased demand for first party cover (and/or more comprehensive policies), as opposed to cover against disputes with third parties, as companies seek to protect their intangible assets. We anticipate the first party cover required would be broad, providing protection against loss of revenue streams from reputational damage and intellectual property to insuring key contracts with important clients. We also expect new insurance products for start-up and SMEs to continue to increase, as often they are quicker to adapt to such risks and will be even keener to secure monetary remuneration in the event they suffer losses resulting from a data breach.

The 'intangibles risk' market (e.g. digital risks) will potentially be larger than the traditional tangibles market…

The 'intangibles risk' market (e.g. digital risks) will potentially be larger than the traditional tangibles market in due course due to the myriad of repercussions resulting from a cyber-breach. Losses resulting from a data breach consist of only one aspect of the intangibles risk market, and we suspect the EDPR will act as an impetus to a market that is already bubbling. Indeed this is what we are seeing in the US, and it seems reasonable to assume the insurance market in Europe will follow in a similar vein as soon as the EDPR starts to bite. ■

Special thank you to John Farrell from Kennedy's Law for his contributions to this article.

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.

Mysteries of the cloud

More and more companies have started to use the cloud to help build products without the additional cost of building an expensive infrastructure.

By doing this, companies are able to launch products quicker and outsource data-centre management to focus on more important core business matters and drive demand.

Recently, many companies in the media space have been utilising the cloud for exactly these reasons. Well-known names such as the FT, The Guardian, BBC, ITV and Channel 4 have moved parts of their business to cloud service providers for various reasons, including to speed up customer access to programmes and services. The financial services sector has also seen an uptake in the number of firms using cloud providers. These and other industry sectors and others see the cloud as a great opportunity to better service their clients in a cost effective and flexible way, however it is important to consider the cyber exposures associated with cloud usage.

When using a third party, especially one that has a multitude of your company data, it is essential to do your due diligence by: researching the provider's cyber exposure by questioning their security measures, identifying what contingent plans they have in place

should they experience an outage, and importantly, negotiating how liability will be allocated in the event of a breach. If they suffer from an intrusion, will they be able / liable to indemnify your company? There are question marks over the safety of cloud and its providers, though generally its track record has been quite good.

Ensure that you are factoring in liability caps with your cloud provider in your cyber risk assessment. Discuss the various additional exposures with your broker and create a cyber insurance policy that covers you should the provider be breached. Remember it is your company that faces customers and the press. What will the reputational harm be to you, should your cloud provider be breached? ■

TOP TWEETS

Britain's stance on cyber crime is like driving a car without airbags perspective
http://buff.ly/1LzEzwO

More companies form data breach response plans
http://buff.ly/1MfO9qG

Cyber insurance uptake nearly triples: Survey
http://buff.ly/1MUHI8D

TalkTalk should have reported cyber attack sooner, says Information Commissioner
http://buff.ly/207XDdu

Don't Strangle the Cyber-Insurance Market in its Cradle
http://buff.ly/1PMXojE

What does the new EU data protection regime mean for datacentres and cloud service operators?
http://buff.ly/1LQFb31