Cyber Insurance, Privacy and Data Security Newsletter - May 2017

Published 12 April 2017

Welcome to the latest edition of our Cyber Insurance newsletter. This month we'll be considering:

- The "significant and growing" risk of cyber threats, as outlined by a recent report by the National Cyber Security Centre and the National Crime Agency;
- The large scale impact of attacks on Industrial Connected Devices;
- The Internet of Things and the rise of Botnets;
- "More aggressive and confrontational" cyber crime.

We also bring you a link to a short video about why businesses need cyber insurance, produced by Lloyd's as part of their cyber insurance summit, and a list of forthcoming cyber focussed events taking place in London and the US.

Before we get to this month's news, we would like to ask for a few moments of your time to make sure you register your **vote** in the **Advisen Cyber Risk Awards 2017**. The Cyber Risk Awards are in their fourth year, but the Cyber Law Firm of the Year is a new award recognising innovation and excellence in the provision of Cyber Insurance Law services. This year we have been nominated for Cyber Law Firm of the Year and we are up against some tough and worthy competition.

We would also like to take the opportunity to personally invite you to our upcoming “Creating an Inclusive Workplace” event in the Old Library at Lloyd’s on 24 May. Please do pop along and join us at this networking opportunity. You can find out more **here**.

Cyber threat "*significant and growing*"

A recent report by the National Cyber Security Centre (NCSC) and National Crime Agency (NCA) (the "**NCA Report**") described the cyber-threat to UK business as "*significant and growing*". 65% of large UK firms detected a cyber security breach in the past year according to the government's Cyber Security Breaches Survey 2016 (the "**Cyber Survey**"). Against this background, cyber security combined with effective risk management, is a key priority for businesses in 2017.
Three factors contribute to this increased threat of cyber-attacks. First, the Internet of Things (IoT) and the progression towards an ever increasing number of internet connected devices provides hackers with more attack vectors than ever before. Secondly, hackers are learning from each other and sharing their knowledge. Thirdly, the technical expertise required to carry out cyber-attacks is declining, as DDoS (distributed denial of service) and malware can easily be obtained on the dark web.

Attacks on Industrial Connected Devices

Industrial connected devices are a prime target for attackers. Not only can they steal intellectual property or collect competitive intelligence but they can also disrupt critical infrastructure on a large scale. An attack on Ukranian energy distribution companies in 2015 resulted in electricity outages for approximately 225,000 customers. This attack was achieved by spear-phishing emails with malicious Microsoft Word attachments containing BE3 malware.
The malware was used to gain access to the business networks of the electricity supply companies and disconnect electricity substations. This exemplifies the very real impact cyber-attacks can have on industry on a large scale, and the NCA Report predicts that such attacks will increase in 2017.
A recently published **report** by Lloyd's, "Future Cities: Building Infrastructure Resilience", highlights the rise of smart technology for city infrastructure and how critical economic and financial services rely on such technology. This presents the very real threat of cyber-terrorists targeting ICT systems to harm or shut down critical national infrastructures. Attacks of this kind can clearly have a devastating impact on local and global economies.

The Internet of Things and the rise of Botnets

As devices become increasingly internet-enabled and accessible, their security measures continue to lag behind. As we have seen with the recent **CloudPets breach**, many products have inadequate security software and are vulnerable to being accessed remotely. Botnets are increasingly being used to mount DDoS attacks on insecure internet connected devices, such as webcams, digital video recorders (DVRs), CCTV and smart meters.
The NCA Report refers to the fact that the Shodan search engine (a search engine that lets a user find specific types of

computers that are connected to the internet) reveals more than 41,000 units of one insecure model of DVR were connected to the internet in January 2017.
The **DDoS attack on Dyn** in October 2016 provides an illustration of the widespread impact of these attacks. Multiple DDoS attacks targeted systems operated by Dyn causing major internet platforms and services to be unavailable to large numbers of users across Europe and North America. The attack affected a vast amount of services from Amazon and Twitter to Netflix and Spotify. It is believed the activities were executed through a botnet consisting of a number of internet connected devices which had been infected with the Mirai malware (the "**Dyn Attack**").
The significance of the Dyn Attack is that the hackers targeted part of the Internet's domain name infrastructure ("**DNS**"). DNS providers operate by translating human readable domain names into IP addresses, helping users find the websites they are looking for. The NCA Report highlights that that we should be prepared to see more such attacks, possibly on a larger scale, and potentially targeting website hosting and database servers.

Cyber Extortion and Ransomware

The NCA Report also emphasises the changing nature of cybercrime and that it is becoming "*more aggressive and confrontational*". Extortion and ransom demands through DDoS attacks or following data theft are on the increase. Internet connected devices again provide an opportunity for hackers as ransomware can target devices containing personal data. The increasing proliferation of wearable technology including smart watches and fitness trackers all present opportunities in this regard.
In January of this year Lloyds Bank was subject to a ransom demand by hackers following DDoS attacks. Some bank customers experienced problems in accessing their online banking portals and outages continued to be reported by customers over two days. The Lloyds Bank website had been overwhelmed by millions of requests in the denial of service attack.
Businesses are being increasingly targeted by cyber criminals because, put simply, they follow the money. Phishing email attachments are a quick and easy delivery vehicle for ransomware. Attackers can reach individuals directly by email and trick them into triggering a ransomware payload, commonly hidden in Microsoft Office documents or JavaScript attachments.
Ultimately the cyber threat to UK businesses is ever increasing, particularly as hackers develop new variants and methods with which to target businesses. Businesses need to regard cyber security as a priority and should have risk management strategies in place to prepare and rehearse for cyber and data breach incidents.

Head of Cyber & Data Risk, Hans Allnutt supports Lloyd's cyber insurance summit

DAC Beachcroft's Head of Cyber & Data Risk, Hans Allnutt, was delighted to support Lloyd's cyber insurance summit and to feature in its new video on cyber security, alongside Inga Beale, CEO of Lloyd's, Baroness Neville-Jones, Former Minister of State for Security and Counter Terrorism and other experts. To watch the video, which explains why businesses should be looking at cyber insurance, click **here**.

Upcoming events

Click the below headings to find out more about these events...

Net Diligence Cyber Risk Summit, London, 9 May 2017
Head of Cyber & Data Risk, Hans Allnutt, is an advisory chair and moderating a session on GDPR at the Net Diligence Cyber Risk Summit in London tomorrow.

Net Diligence Cyber Risk & Privacy Liability Forum, Philadephia, 5-7 June
Head of Professional Liability, Patrick Hill will be discussing "GDPR – Is international compliance illusory?" at 11.30 on 6 June.

Net Diligence Conference, Santa Monica, 10-12 October 2017
Hans Allnutt will speak on GDPR and European Cyber Developments in California in the Autumn. More information coming soon.

ABI 2017 Data Conference, London, 19 October 2017
Emma Bate and Rhiannon Webster will present on the Internet of Things and GDPR at this one day event.

UK Developments

Click the below headings to read more on each of the developments...

- **The UK courts take on Subject Access Requests and hand down 4 significant decisions on this issue**
- **The UK courts confirm that data protection claims can now be brought alongside defamation claims**

Updates from across the world

Click the below headings to read more...

- Argentina - Argentina issues draft data protection bill
- Australia - Mandatory data breach notification act passed by parliament
- Czech Republic - Data controllers not able to contract out of their duties
- France - CNIL launches a second public consultation on the GDPR
- France - French data protection authority publishes six-step methodology to comply with GDPR
- Ireland - High Court reserves judgment in Schrems case
- Italy - Italian DPA decision regarding the employer's remote controlling of the employees' work activity
- Italy - Italian DPA issues EUR 11 million fine for breach of personal data protection code
- Portugal - Guidelines on the access to personal data contained in workers' pay slips in the context of an enforcement procedure
- Russia - Personal data violations bill introduces civil offences for violation of data subjects' rights
- Serbia - Model of GDPR compatible law on protection of personal data introduced
- Spain - The obligation for data controllers to register files containing personal data will disappear in Spain with the new GDPR
- United States - Record number of data breach notices in New York in 2016

Authors

Hans Allnutt
London - Walbrook
+44 (0) 20 7894 6925
hallnutt@dacbeachcroft.com

Rhiannon Webster
London - Walbrook
+44 (0)20 7894 6577
rwebster@dacbeachcroft.com

Patrick Hill
London - Walbrook
+44 (0)20 7894 6930
phill@dacbeachcroft.com

DAC BEACHCROFT