October 2016

Hacks, cyber-attacks and simple human error: protecting personal data after TalkTalk

You may recall our briefing about cyber-security last Autumn. The UK data protection regulator (the ICO) has now completed its investigation of the TalkTalk cyber-attack, and it makes difficult reading for TalkTalk.

£400k fine imposed

The ICO has fined TalkTalk £400,000 (or £320,000 if paid by 1 November). This is the highest fine yet levied by the ICO. The ICO press release comments that TalkTalk had security failings which allowed the attacker to access customer data (including bank account details) "with ease", and that TalkTalk could have prevented the attack in October 2015 if it had taken basic steps to protect customer's information.

Recently appointed Information Commissioner, Elizabeth Denham, commented: "Hacking is wrong, but that is not an excuse for companies to abdicate their security obligations. TalkTalk could and should have done more to safeguard its customer information...Cyber-security is not an IT issue, it is a boardroom issue."

In our previous item we pointed out that hacking often succeeds because of basic human error. So it has proved with TalkTalk. The ICO found that in spite of TalkTalk's expertise and resources, when it came to the basic principles of cyber-security, TalkTalk was found wanting. The ICO report says: "For no good reason, [TalkTalk] appears to have overlooked the need to ensure that it had robust measures in place..."

> *"For no good reason, [TalkTalk] appears to have overlooked the need to ensure that it had robust measures in place"*
>
> ICO report, October 2016

How did TalkTalk get hacked?

The attacker used a common technique known as SQL injection (to which known defences exist) to access data via three webpages which proved vulnerable – TalkTalk was unaware of the webpages, inherited in a 2009 acquisition, or that they enabled access to a database holding customer information. Moreover, TalkTalk was

unaware that the installed version of the database was outdated, was no longer supported by the provider and was affected by a bug to which a fix was available. That fix (well publicised in 2012) would have prevented the successful attack. The company also suffered two earlier attacks in July and September 2015 (of which at least one was successful) which it failed to respond to.

What could TalkTalk have done better?

According to the ICO, TalkTalk should have been able to:

- Spot the web pages it had overlooked;
- Secure or remove them;
- Ensure adequate testing and monitoring (and react to threats quickly); and
- Apply the bug fix available since 2012 or upgrade to a newer version of software unaffected by the bug.

Previous highest ICO fines

- £250,000 on Sony Computer Entertainment Europe for failure to take adequate measures to protect against hacking (2013)
- £325,000 on Brighton Sussex University Hospitals NHS Foundation for failure to wipe hard disks containing sensitive patient data (2012)

These risks were well known by 2015 and the errors were classic stuff, so it is not surprising that a fine has resulted. We regularly see similar errors. Nonetheless, the ICO response is unusually forthright and, with the size of fine imposed, may mark the start of a more deterrent approach from the traditionally light-touch regulator – though the cost of resolving the incident, which TalkTalk has put at about £60m, might itself be quite an incentive to keep security up-to-date. But it is a reminder of the importance of proper cyber-security for all businesses, no matter how large or small.

Higher fines in future?

As a footnote, it should be added that from May 2018 the new General Data Protection Regulation will have effect. While the basic obligation to ensure "appropriate" data security remains unchanged, the level of potential fines will increase substantially – to a maximum of the higher of 4% of worldwide annual turnover and Eur 20,000,000.

HOW WE CAN HELP

If you would like to discuss any of the issues raised in this briefing, please speak to one of the contacts listed below, who are all experts in technology and data privacy law.

10 Snow Hill
London EC1A 2AL
T: +44 (0)20 7295 3000
F: +44 (0)20 7295 3500
www.traverssmith.com

Dan Reavill
Partner, Head of Technology Sector Group

E: dan.reavill@traverssmith.com
T: +44 (0)20 7295 3260

Louisa Chambers
Partner

E: louisa.chambers@traverssmith.com
T: +44 (0)20 7295 3344

Alistair Wilson
Consultant

E: alistair. wilson@traverssmith.com
T: +44 (0)20 7295 3345

James Longster
Senior Associate

E: james.longster@traverssmith.com
T: +44 (0)20 7295 3496

"Travers Smith LLP 'provides clear advice and pragmatic solutions' to clients such as Trainline, LK Bennett, Nature Delivered and Prudential. The team handles [data protection] breaches, audits and compliance and outsourcing contracts. Practice head Dan Reavill is 'excellent'."

Legal 500 (2016)