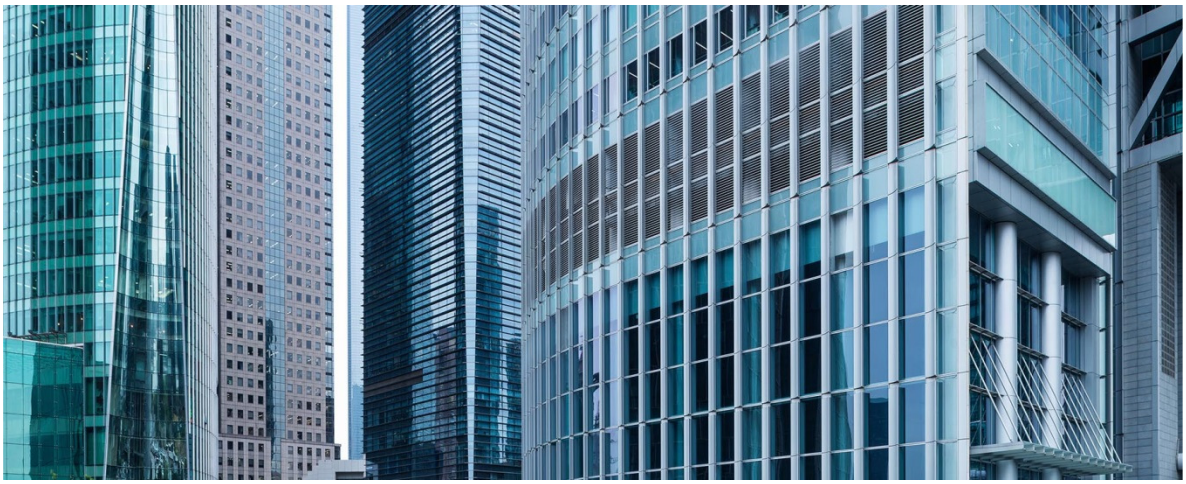

Summer 2015

Hacks, other cyber-attacks and simple human error – protecting personal data

As the uses to which personal data is put have become greater and more sophisticated, so have the risks of something going wrong.

We are seeing many more deliberate attacks and regularly advise clients on containment and mitigation in the aftermath of security breaches, including data theft involving malicious hacking. And this isn't just confined to users of "Big Data". Attacks can be very sector specific and frequently exploit weaknesses in small businesses.

The legal consequences are also multiplying e.g. larger fines levied by authorities, potentially more claims for damage by individuals whose data has been lost, misused or taken (as a result of a current landmark case) and the introduction in the next year or so of new and more onerous European data protection legislation. Of course legal liability for loss isn't automatic, and you are in a much better position to defend against regulatory attack if you have taken diligent preventative steps; an aspect the regulators are focusing on to improve good practice. Here are three of the more common issues that we have seen recently – and some of the steps regulators have recommended to protect your systems and the personal data which you hold.

Hacks and cyber-attacks

Earlier this summer Avid Life, owner of adultery website Ashley Madison, suffered a major and sophisticated cyber-attack, in which 9.7 gigabytes of customer data appears to have been accessed and posted online.

Preventative steps

- Adopt, keep up to date and enforce a data security and retention policy, including regular review of whether any of the data you are holding has become historic or unnecessary
- Don't ask for any personal data that you don't need
- Consider engaging a professional technical security firm to review your encryption strength and system security
- Mobile devices can be more vulnerable than traditional computer hardware – consider whether it is necessary/appropriate for your staff to use mobile devices to access your systems
- Consider taking out insurance against cyber-attacks and data loss

Theft or loss of laptops/memory sticks

North East Lincolnshire Council was fined £80,000 after an unencrypted memory stick containing data relating to children was lost.

Preventative steps

- Make sure that laptops and mobile devices do not contain full copies of all databases, unless access to that quantity of data is absolutely necessary
- Routinely review the physical security of your offices and server rooms
- Have (and enforce) staff system access policies
- Regularly train staff about the importance of data protection and security

Loss or misuse of data by service provider

In March 2015 the Daily Mail reported that salesmen at data broker companies are claiming to have "access to the salaries, investments and pensions of a million people" and that this information is "being sold for as little as 5p". Many companies are dependent on some form of outsourced service provision which requires personal data to be transferred to the provider.

Preventative steps

- Carry out proper due diligence on all service providers who may process data on your behalf
- Make sure that you have data processing contracts (including appropriate non-disclosure provisions) in place with all service providers who may handle personal data, as required by law
- Don't give service providers copies of all of your data when they only need part of it
- Prohibit sub-contracting by your service providers, unless your consent is first obtained and the sub-contractor demonstrates appropriate security
- Consider asking for rights to audit service providers' data protection compliance, and use those audit rights

HOW WE CAN HELP

If you would like to discuss any of the issues raised in this briefing (whether about how to devise and implement suitable policies, about handling damage limitation after a security breach or any other aspect), 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
Head of Technology Sector Group

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

Louisa Chambers
Senior Associate

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

Deborah Lincoln
Senior Counsel

E: deborah.lincoln@traverssmith.com
T: +44 (0)20 7295 3293

James Longster
Senior Associate

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