4 May 2015

THE SCOTSMAN
SCOTLAND on SUNDAY

Between the Lines

Could data protection be the new health and safety?

Money and reputation are as risk with a data breach, writes **Laura Irvine** and **Paul Motion**

FOR businesses in Scotland today, health and safety is a prominent feature on the operational agenda. Prosecution resulting from breaches of the Health and Safety at Work Act 1974 (HSWA) can result in reputational damage and costly fines, therefore most businesses are clear about what is expected of them in terms of satisfying the Health and Safety Executive (HSE) and keeping their employees and others safe.

However, are businesses as informed and compliant when it comes to data protection, and do they attach the same amount of importance to minimising the risk of breaches? The Information Commissioner's Office (ICO), which enforces the Data Protection Act 1998 (DPA), is a relative newcomer in comparison to the HSE, but it is making its presence known to organisations, with the ability to impose fines of up to £500,000 for a data breach.

Whether resulting from cyber-crime or human error, breaches can severely dent customer and investor confidence, further compounding the financial losses incurred by interruption to business and the payment of fines. A 2014 security survey suggested the average cost of remedying a serious security breach for large firms was between £600,000 and £1.15 million, while SMEs can expect to lose between £65,000 and £115,000.

While some could argue the level of fines imposed under the DPA for loss of personal data is already disproportionate when compared to those imposed for the loss of life under the HSWA, a new EU General Data Protection Regulation could see regulators given the power to impose fines of up to €100,000,000 or 2 per cent of global annual turnover.

The new EU Regulation which comes into force over the next couple of years is also likely to compel organisations to notify their regulator of a serious data breach, and may also require companies over a certain size to have a data protection officer.

It vital managers assign the same importance to DPA compliance as they do to adhering to the Health and Safety at Work Act. Any organisations that are data controllers must have suitable and sufficient policies to ensure data is handled in compliance with the eight Data Protection Principles.

With 40 per cent of data breaches arising from employee error, training staff and monitoring their compliance is essential. Third party processers handing personal data on behalf of a company must be contractually tied into similar standards, as the data controller is ultimately liable.

Training staff and monitoring is essential

The ICO expects to see a Privacy Impact Assessment for any project impacting personal data, for example installing CCTV – this could be characterised as a DPA risk assessment. Minimising the risk of cyber-attacks as far as possible is strongly encouraged, with failure to do so likely to result in enforcement action being taken.

If your organisation experienced a health and safety breach, you would follow a well-defined process. Data breaches are little different but frequently information is volunteered and statements made during an investigation that should first have had a professional eye cast over them.

The message is: make sure data protection compliance is on the board room agenda and that you have effective policies and procedures to ensure compliance well before the EU Regulation comes into force. Since "we were the victims" cuts no ice with the ICO if your systems are compromised, now would be a good time for your organisation to investigate cyber-risk insurance.

● *Paul Motion, partner, and Laura Irvine, associate, of BTO solicitors' Data Protection Defence team.*