

## Data Protection 2009 - Am I now in the firing line?

### ***The Data Protection Act 2009***

It is my considered view after almost 30 years working in the field that although we do not formally have a new data protection act the Data Handling Regulation published last year by the Cabinet Office and the way in which the Data Watchdog – The Information Commissioners Office (ICO) - have expressly said they are going to apply them (and indeed have) makes this point moot. To all intents and purposes we now have a new much tougher Data Protection Regime – which may as well be The Data Protection Act 2009.

### **New Legal Roles and Responsibilities**

Not least because the Data Handling Regulations clarify create new legal roles and responsibilities – principally that of the SIRO (Senior Information Risk Owner). Historically lines of responsibility have been unclear where data breaches are concerned and this has been tackled by the creation and de-facto imposition of this new role and title.

### **What is a SIRO... Who is a SIRO?**

Most of the people who are currently SIROs are unaware of this. The regulations make it clear that the top person (CEO, Headmaster, etc) of each organisation is – by default – the SIRO. In effect this means that the responsibilities fall on them and in the event of a data breach they will be held to account.

### **Am I a SIRO?**

If you are the top person in your organisation (or ultimately considered by a judge and/or the ICO as such) then you are a SIRO whether you know it or not. The principle that 'ignorance of the law is no excuse' applies. In the final analysis it is you that the ICO and the judiciary will come to in the event of a breach.

### **Can I delegate this responsibility?**

This is unclear as it has yet to be tested in court (as of this writing Mar2009). What you can do is delegate the work involved and appoint a suitably qualified officer to report to you on this clear responsibility. It is likely that in the event of a court case or a dialogue with the ICO clear evidence of a plan and appropriate measures can go a long way towards a credible defence.

### **Does this apply to my organisation?**

The regulations are framed firstly as to be directly applicable to central and local government – but it is very clear that the ICO intends to apply them as widely as possible as soon as possible. BECTA for example have issued advice to the education sector that they do indeed apply to schools and all other educational institutions and it is clear that the legal profession will be expected to comply within months rather than years. Taken together it is clear that this compliance pressure will move quickly through supply chains - since it's clear that contractors must expressly confirm / demonstrate compliance.

Meanwhile the ICO has made it clear that breaches will be dealt with within this framework in any case and leniency has been expressly ruled out – whether the compliance pressure has reached your organisation or not.

### **What are the MMMs – Mandatory Minimum Measures – I hear about?**

These are the keystone of the new approach and are aimed at making explicit the risks and ensuring that they are addressed - briefly summarised:

- Personal data **MUST** be suitably encrypted in transit. The vast majority of the breaches over the last year and more have been from careless use of memory devices such as memory sticks and from unencrypted laptops lost or stolen.
- Documents **MUST** be clearly labelled with the appropriate Impact Level – explained below.
- Remote access **MUST** be secured by suitable encryption and strong authentication.

The ICO has made it crystal clear that if a device is stolen for example – from an employee’s home say – then the responsibility for this breach rests with the organisation and it’s SIRO. It has backed this up with action by fining the Nationwide Building Society almost £1m in precisely these circumstances.

It has also censured and compelled the head of a number of errant organisations to sign a legal undertaking to uphold the regulations in future – including the head of the Home Office and of an NHS Trust.

### **What is Impact Level Labelling?**

The regulations define a system of ‘Impact Levels’ which are drawn from a larger and long standing scheme used in government and the intelligence services (see

[http://www.cabinetoffice.gov.uk/media/cabinetoffice/csia/assets/dhr/cross\\_gov080625.pdf](http://www.cabinetoffice.gov.uk/media/cabinetoffice/csia/assets/dhr/cross_gov080625.pdf) page 8)

These broadly chart the level of impact on a person or people should the document be breached. Here’s a flavour:

### **Impact Levels**

Impact Level 0: Public information.

Impact Level 1: Trivial information about an individual that would be easy to obtain as it’s already in the public domain – say from a Google search.

Impact Level 2: **Protect**. ‘General Citizen Data’ – which would have some impact on an individual if breached – advice cites passwords and usernames.

Impact Level 3: **Restricted** (e.g. NHS Confidential). This would have a significant impact on the individual if breached and would include health records, crime records and likely HR and financial records for example.

Impact Level 4: **Confidential**. This would have serious implications for an individual if breached – and cites information concerning someone on a witness protection programme as an example.

It's also clear that the severity of any breach is to be measured also on the quantity of data (i.e. the number of individuals potentially affected). So a moderate breach of a single record is considered less severe than for a 100 or more records for example.

### **What do I need to do if I am a SIRO?**

You need to understand the responsibility that you now clearly have as a result of these changes, assess your risk and form your plan of action. It may be that your risk is low/acceptable – but it is up to you to make an assessment and be prepared to defend your decision if necessary. The following cycle is often used as a guide or pattern to help with this process

1. Measure the risk
2. Form a plan to limit the risk
3. Implement the plan – and after a suitable period return to step one to review the plan and the risk.

### **What do I need to do if I'm not a SIRO?**

Even if you are not a SIRO you still have responsibilities. While the ICO won't (as far as we know) address you – rather your organisation via your SIRO - it's likely that your organisation will hold you accountable and if necessary take disciplinary action in the event of a problem for which you hold some responsibility.

It's not yet clear to us what stance a court might take in the case of gross negligence for example – but it seems likely that it may well be a dim view. It seems even more likely that in the case of an industrial tribunal there would be support for an organisation that took appropriate action against an employee who had acted against the company's interests in this regard – especially since the organisation and the SIRO necessarily depend on employees – having taken appropriate measures – to uphold and implement them.

### **Recommended Actions**

It is probably a good idea to start drawing your SIROs attention to this information if they are not already conversant with it as a means of protecting your organisation. It is clear that any organisation can be severely affected (by fines and loss of reputation etc) – in some cases so severely that they are unlikely to survive. Especially in the challenging economic conditions in which we now find ourselves.

These conditions in turn pose new risks – there is greater temptation for employees to use company data for their own gain – especially departing employees. Recent research has established that this is already emerging as a clear pattern in fact.

## **Help**

For those used to assessing risk and already in the cycle described this information may contain few or no surprises – but may still require a reassessment – looking at the latest tools and best practice to counter their risks.

For those new to this topic it can appear daunting. Help is available as well as tools to enable you to assess and reduce your risk and be ready to meet compliance.

Contact 0844 8844941 for more.

© **Copyright Barry E James, March 2009** (V0.03)

See also in this series:

[\*\*The five things every manager needs to know to survive 2009\*\*](#)