

Article:

DLP - Five things every manager needs to know to survive 2009

eCrime is threatening UK businesses

eCrime has become endemic and poses a real and present risk to businesses and other organisation across the UK – and worldwide.

Cyber criminals want to steal the kind of data you have (and are prepared to groom employees to do so) because they can turn them into hard cash. The problem has become more acute because of the recession as employees – particularly those being made redundant or under financial pressure - are key targets.

Your data – both personal data relating to your employees, customers/clients and partners and you commercially valuable data (payroll, prospect and customer lists, price lists, orders, IP etc) - are a target because there is a ready market for them and the chances of being caught let alone charged or convicted are vanishingly small – the authorities are playing catch-up.

Zero% Chance of being caught?

This has become an acute problem very swiftly fuelled by a recession which has put financial pressure on employees and provides a keen temptation to those leaving or being made redundant to sweeten the pill – and their chances of another job – by taking away information that could make them more valuable and attractive to another potential employer. Again the chances, overall, of them being caught or held to account are – in most organisations – negligible.

2009

Meanwhile we have a new situation – the Data Protection act and the way it's applied has changed radically, with the Data Watchdog, The Information Commissioner taking a new stance - seeking prosecutions and handing out large fines to organisations failing to protect people's data.

Last year was the year of data losses with millions of people's personal details gushing out of public and private sector organisations – companies and government bodies like HMRC and PA Consulting.

This year is the year the recession really bit. and has matters worse. A recent survey revealed that 80% of employees leaving or being made redundant would take company data with them without a second thought – using the company's data for their own enrichment. It used to be called stealing – it's now 'white collar crime'.

dBay

There is an established and ready market for this data and criminals are looking to actively groom disaffected employees to get it. 'DarkMarket' was recently revealed as an FBI sting operation which mirrors other such markets for stolen data around the world – personal and commercial data.

Like earlier crime sites, [DarkMarket](#) allowed buyers and sellers of stolen identities and credit card data to meet and do business in an entrepreneurial, peer-reviewed environment. Products for sale ran the gamut from specialized hardware, to electronic banking logins collected from phishing attacks, stolen personal data needed to assume a consumer's identity ("full infos") and credit card magstripe swipes ("dumps"), which are used to produce counterfeit cards. Vendors were encouraged to submit their goods for review before offering them for sale.

See <http://blog.wired.com/27bstroke6/2008/10/darkmarket-post.html>

£Data.00

Data now has a monetary value. Laptops are still widely stolen but the contents often have more value. It's obvious when a laptop is stolen as it can be seen to be missing – but most organisations would not know if their most valuable and sensitive data had been copied.

While the loss of business if, for example, a customer list, order book – or other sensitive information - is taken can pose a risk to many organisations – particularly small ones – another related risk has emerged.

Large Fines & other 'Enforcement action'

As well as the threat of data going missing is the threat of 'enforcement action' or worse from the IC (Information Commissioner) – the data watchdog – who has new teeth.

The IC has now committed his organisation to prosecuting not just losses that are reckless or criminal but those that arise from neglecting to batten down the hatches properly.

So much so that although technically the data protection law hasn't changed it may as well have. In effect we now have the Data Protection Act 2009.

The Data Protection Act 2009

It is clear 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 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 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.

For more information on the Data Handling Regulations see the next paper in this series... "Data Protection 2009 - Am I now in the firing line?" at www....

Recommended Actions

There are two sides to this new risk:

- Direct threat to the organisation through data loss – losing business to competitors, reputation damage etc
- Indirect threat of action by the authorities – large fine and/or reputation damage.

Both can be tackled by taking sensible measures – which need not be costly – to assess and reduce risk using this approach:

1. Assess the risk
2. Take action to reduce the risks
3. Return to step 1 to review the effects and whether the risk is now acceptable (and compliant)

The two most important components to consider are

- People – it's important to make every employee handling data aware of their responsibilities and that they will be held accountable for them
- IT – Tools now exist to make the information available for the above and where necessary police compliance with company policy.

We produce some of the leading software able to do both – with the minimum of hassle fuss and cost.

Please see the TakeMeasures Suite at www.TakeWare.co.uk for more information.

See also the other two papers in this series.

Help

For those used to assessing risk and already in the cycle described this information may contain few or no surprise. 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.

Please contact us on **+44 (0)844 8844941** or via www.TakeWare.co.uk for more information.

Summary

- eBay – Your data now has monetary value to others – who want to steal it.
- Disaffected, disgruntled and redundant employees can pose a serious business risk.
- Data Protection 2009 - the landscape has changed and you have been handed a new level of personal responsibility for personal data.
- In a global recession no one doubts that these risks will sink some companies and cripple some others.
- Yours does not have to be one of them - there are some easy to implement measure that can drastically lower your risk.

Please see the TakeMeasures Suite at www.TakeWare.co.uk for more information.

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

See also in this series:

[Data Protection 2009 - Am I now in the firing line?](#)