Breaches of security

The Information Commissioner recently issued huge fines for data protection breaches. Edward Murray reports on additional costs that could well flow from new notification laws.

THERE WAS A STING in the tail end of 2010 for Hertfordshire County Council and Sheffield-based A4e when they were fined £100 000 and £60 000 respectively by the Information Commissioner's Office in late November, following serious data breaches. The fines were the first financial penalties doled out by the ICO since its powers were beefed up in April 2010 and serve as a strong notice to companies across the UK that it will cost them dearly if they do not look after their data properly.

In addition to the hoped-for deterrent effect of fines, there are also further potential changes to companies' responsibilities on the immediate horizon when it comes to managing sensitive data. And the insurance market is working hard to develop policies that cover the risks effectively and educate companies about the liabilities they face, not to mention having to get their own houses in order as holders of extensive personal customer data themselves.

Mandatory notification

Perhaps the biggest emerging issue is that of mandatory disclosure. Essentially, this is a requirement for any organisation to swiftly put up its hands, admit there has been a data breach and inform all of those affected.

California was the first state in the US to introduce mandatory disclosure back in 2003 and since then virtually every other state in the union has followed suit. European countries such as Germany and Portugal have also got in on the act and introduced notification responsibilities.

So, just how long will it be before such legislation washes up on our own shores? According to Dawn Simmons, senior underwriter for professional lines at XL Insurance, not long — as increasing noises are already being made about introducing a European Union-wide notification regime. Writing for *Post Europe* in October 2010, she said: "The increased power of EU data protection authorities and stricter punishments levied on violators of existing EU data protection laws indicates that the EU is seriously considering moving towards a more comprehensive data breach notification regime.

"As society in Europe becomes increasingly reliant on online services there is growing awareness of data protection issues among the European public and increased enforcement of data protection laws. Companies need better measures to safeguard personal data under their control — or risk facing potential damage to their reputation and bottom line." (*www.postonline.co.uk/1736570*)

For some organisations, more onerous requirements will come sooner rather than later. In May, changes to the European directive on data protection will see internet service providers and telecoms companies compelled to notify individuals in instances where there has been a data breach, and some degree of contagion into other commercial sectors seems likely. Banks, general insurers, healthcare providers and retailers will all be in the front line when it comes to extended mandatory disclosure legislation, but at the moment they have time to assess the situation and prepare enhanced risk management mechanisms.

> The EU is seriously considering moving towards a more comprehensive data breach notification regime. Simmons

Kenneth Mullins, partner at law firm Withers, comments: "The thing lurking in the background here is that the EC is looking at overhauling the data protection regime this year and I suspect that, out of that, there will probably be some pressure applied to actually introduce a mandatory breach notification rule across Europe." He adds: "I would not hold my breath that it will arrive in the next year or two, but I suspect there will at least be a serious look at introducing it across all businesses — including insurance and broking."

It seems, therefore, that additional legislation is in the post, but for those other than ISPs and telecoms companies there is little certainty as to just when it will arrive and what shape it will take when it does.

While data breaches may well be on the radar of companies and organisations holding vast amounts of personal customer information, these are by no means the only companies that are going to be affected in the future. Indeed, there are many firms in sectors like manufacturing that believe their business-to-business set up puts them outside of any potential legislation when it comes to data breaches.

However, this is not the case and, when data goes astray, it is not just customer data that is important. It is any personal data; so that of employees counts just as much as that of any customer.

This is a point Iain Ainslie, technology and cyber liability underwriter at Ace Europe, makes: "In the manufacturing arena, companies tend to be B2B with little consumer information on their systems. However, once you look at how many employees they have, then it often becomes a very different matter.

"One person I spoke with said he had 20 000 staff at any one time and he has bank account details, personal information, pension scheme details and all sorts of things. So the risk can be significant."

But why the big drama around the introduction of mandatory disclosure for a data breach? The short answer, as always, is money; the need to tell people that a data breach has occurred costs a huge amount.

The Ponemon Institute was founded in Michigan in 2002 and is regarded as a leading authority on issues surrounding privacy, data protection and information security. It has collated extensive information on the costs associated with a data breach and, in particular, those that come from mandatory disclosure requirements. According to its research, each compromised customer record costs companies a little over $200 ($129) and includes outlays for detection, escalation, notification and response along with legal, investigative and administrative expenses, customer defections, opportunity loss and reputation management. It also factors in costs associated with customer support such as information hotlines and credit monitoring subscriptions.

Bearing in mind that other EU member states may soon be required or choose to follow Germany's example, it is worth noting that studies by the Ponemon Institute also found the average cost of a data breach there rose by 7% in 2009 — to approximately €2.58m ($2.18m) — a figure, according to Ms Simmons, expected to rise higher due to the country's newly passed legislation.

Should mandatory disclosure be introduced in the UK, it must be hoped that companies and organisations are continuously striving to improve their data protection strategies — if earlier findings by the Institute are anything to go by.

In June 2008, it reported that the loss or theft of private and confidential data is endemic among UK firms with almost two-thirds (61%) of marketing professionals experiencing a data breach involving the loss or theft of consumer information over the past 24 months. In 90% of those cases, the loss or theft went unreported since firms felt that they were either not required to, or were unsure whether they had to, report the incident to the affected customer.

While it is, perhaps, difficult to make direct comparison with the US or Germany and transpose the above figures directly into the UK, they do offer a reasonable estimate of just how much mandatory disclosure could cost organisations at a basic level. Ben Beeson, an executive director at broker Lockton, believes that firms should be looking at upwards of £10 and closer to £20 a head when it comes to the baseline cost of notification.

This may not seem a huge amount, but multiply this by a factor of 25 000 compromised records and, all of a sudden, organisations are staring down the barrel of a $500 000 bill. Insurers, such as Beazley, are offering cover that provides protection for up to four million lost records, giving some indication of the scale of the problem that major national and international organisations face.

Policy trigger development

Mr Beeson says: "The big thing that gets companies focused on handling personal data of both customers and employees is the requirement to notify. That is the only way that you get companies to take things really seriously." He believes it will be the need to notify that drives the development of the insurance market further and secures genuine interest in cover from UK firms.

At the moment, many policies are only triggered by a legal requirement. In the UK, therefore, where notification remains voluntary, these policies would not respond to the costs involved when notifying customers. Clearly this is unsatisfactory and, when companies are increasingly being asked to voluntarily disclose a data breach, they need to know that associated costs would be covered by their insurance.

Commenting on the way policies are developing, Mr Beeson says: "The policies that evolved out of the US were initially only triggered by a legal obligation to notify. Clearly that does not work outside of the US and many of these policies have now been broadened to provide voluntary notification — typically, with the underwriter's prior consent to do that."

Ben Maidment, technology, privacy and cyber liability underwriter at Brit, adds: "There is a movement within the insurance market to add voluntary notification costs and, if it is best practice and deemed to mitigate the loss, then we will accept a claim for a voluntary event. That is where many policies are going at the moment. It has really been the trigger for purchase in the US and so, to sell policies in the UK and Europe, it is perhaps something we need to address in a reasonable way."

While it seems that some form of mandatory disclosure will inevitably be cast upon the UK's public and private sectors, there will be significant discussion around the form it should take and the threshold over which firms have to respond.

> If a cleaner has access to the systems because someone forgot to lock the server room, does someone need to notify? Mullins

If firms have to disclose each and every potential data breach, then they are likely to be speaking to customers on a very regular basis and devaluing the impact of the action.

This is a point that Mr Mullins makes when he says: "If there is no materiality threshold to get over, and the actual breach does not have to be significantly serious before you must notify, then people are going to be inundated with these things. Where do you stop? If a cleaner has access to the systems because someone forgot to lock the server room, does someone need to notify?"

He adds that some firms in the US have taken to sending out marketing literature with their mandatory notifications and asks whether this is appropriate or simply damaging to the whole process. "Sometimes using mandatory notification on an ill-thought-out basis can be counter productive as it does not actually raise awareness," he warns. "It just means people are even more jaded when it comes to being told about it."

Whatever form future disclosure legislation takes, the issue is serious enough for insurers to be looking at protecting themselves from the threat of a data breach. Groupama Insurances, for example, is currently in the process of securing cover to respond in such an event. David Ragan, group compliance officer, comments: "If we had a hardware problem then we would be fine as we have back-up systems already in place. If we had a location failure, there are warm sites we could go to at a moment's notice. But our gap analysis has identified a complete collapse on our data as being our biggest potential risk."

The internal implications that such a collapse carries do not relate specifically to business interruption costs, but also the threat of data going astray and all of the costs of notification, investigation and contact with the regulator that would ensue.

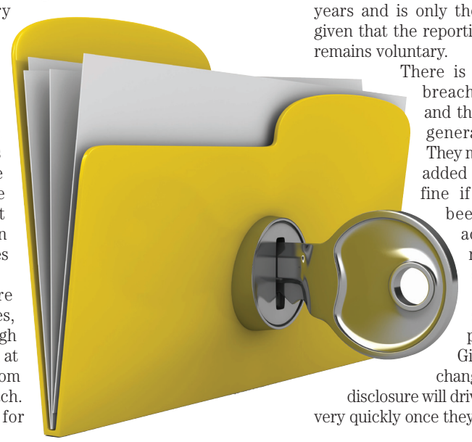
Threat of litigation

The bottom line is that for an individual to sue a company over a data breach they have to be able to prove there has been significant damage or distress suffered. This is not something that is easy to do and, to date, there have been very few if any cases where individuals have materially suffered on the back of their data being lost. As such, the threat of litigation is viewed by most as minimal and — until notification becomes mandatory — Mr Beeson says it will be difficult to encourage UK firms to buy cover.

He comments: "Selling this insurance in the UK today is still incredibly difficult as not enough companies see enough of a risk to warrant paying to transfer it off their balance sheet. Consequently there is more limited scope for insurers here but, as soon as notification obligations come online, I expect to see the market evolve as it has done in the US."

At the moment, the market remains focused on organisations that either have subsidiaries in the US or that are working for US firms that have insisted they carry the cover. This is particularly the case where a US firm has outsourced the processing of customer data or transactions to a third party and is not prepared to carry the liability should the third party suffer a data breach.

This, therefore, may not be an issue that currently looms large on the risk management screens of most UK organisations, but it is quickly growing in importance. In May 2010, the ICO reported it had received voluntary notification on its 1000th data breach. This tally had been reached in less than three years and is only the tip of the iceberg, given that the reporting of these incidents remains voluntary.



There is no doubt that data breaches are widespread and that the costs they can generate are significant. They may also come with the added sting of a regulatory fine if organisations have been found to have acted deliberately or negligently in losing data and failed to have reasonable systems in place to protect themselves. Given this backdrop, the changing demands around disclosure will drive this market forward very quickly once they arrive. **POST**

» IS TOUGHER LEGISLATION NEEDED?
For all the latest developments in this area
www.postonline.co.uk/tag/risk-management