RegulatoryStrategies

Data breaches - don't wait for the accident to happen.....

This year's Information Commissioner's Annual Report in the UK again placed lenders at the top of its complaints' table, accounting for 15% of all complaints received. Coupled with other financial services' related sectors, including insurance and debt collection, this rises to 21%, and when general business complaints are added to this we reach 32%, way ahead of central and local government, health and telecoms combined.

So our industry is certainly high profile in the eyes of not only the financial services sector regulators, but also the Information Commissioner's Office.

The Information Commissioner's Office has recently issued new guidance for small businesses which clearly outlines what its expectations are in terms of protecting customers' and employees' data. And there are some critical pointers in this for organisations of all sizes and sectors.

And meanwhile, negotiations about the draft European data protection regulations are bubbling away – whatever the outcome, there is little doubt that a much stricter regime in terms of safeguarding personal information is on the horizon.

The ICO's 'IT Security Guide for small businesses' clearly reiterates the advice the ICO, and the Financial Services Authority, have been issuing to all businesses under their jurisdiction for a number of years. It emphasises that a breach of legislation can incur a fine of up to £500,000 as well as resulting in untold reputational damage. The number of fines that have recently been imposed shows that the ICO will take action where it deems it appropriate – the total amount of fines between July 2011 and July 2012 equated to £2 million.

Businesses are expected to have physical security to protect against criminal activity, the appropriate levels of anti-virus and anti-malware products, robust access control processes for employees. Underpinning these levels of protection should be robust and formalised policies including an incident management policy. Even this would be deemed inadequate if staff are not trained in policy compliance and have an awareness of their responsibilities in handling and protecting customer data.

If a data breach occurs (and the ICO has always been clear that it understands that no organisation is invulnerable – the ICO has recently confirmed that data breaches have increased by 10 times over the last five years), organisations are liable to face regulator action if they do not have the above in place. However, as the regulation stands at the moment, businesses generally get away without having these safeguards in place unless something goes wrong and the missing defences, awareness training and policies are visibly missing.

The proposed new EU regulations, whatever the final detail, will undoubtedly mean that the regulator will have strengthened auditing powers. Protecting customer data will no longer be an 'insurance policy' to protect businesses just in case a data breach occurs. It will be a 'must have' for any organisation processing personal data.

Businesses will be expected to have data protection awareness and considerations integrated into their activities to the extent that many companies are likely to be required to have a data protection officer. Data breach reporting will, in some form, become mandatory to both the data protection authority and to the customers who have been impacted. Fines are likely to be far less down to the ICO's discretion but specified within the legislation.

The new regulations may still not come into force for a few years but embedding policy and awareness into an organisation is not something that happens over night and can be an unwelcome distraction from business as usual.

The reality is that the ICO's expectations of organisations really just reflect what is common sense and good business practice. Many organisations already go a long way to ensuring that customer data is protected but what often happens is that, where data protection awareness exists within a business, this is not reflected in formal policies. The flipside can often be that those companies who have well-documented policies and procedures haven't made sure that staff are well-versed in them.

The best approach is to act now – make sure that you already comply with what the ICO and your customers would expect. That way data breaches can be prevented and, should one occur, your business has a plan to react quickly to it and mitigate or limit the impact. It will also save cost and the concentrated use of resource in the not-too-distant future when the new data protection regulations come into force, the reporting of breaches ceases to be discretionary and there is a real potential for your organisation to be audited to confirm that those safeguards are in place.

Ask yourself whether you have data protection policies in place, an up to date privacy policy compliant with the new cookie regulations, an incident management plan, a retention strategy, robust contracts in place with third party suppliers that include data protection clauses. Are you and your staff equipped to respond promptly to a subject access request? Do all staff fully understand their data protection responsibilities and have they received adequate training?

If the answer is 'no' to any of the above then it unlikely that the ICO's expectations would be met and, when the new regulations add to our ever growing compliance requirements, there will be a legal requirement to put these things into effect.

Don't wait for the accident to happen.....

Helen Lord
Director
Regulatory Strategies
Helen.lord@regulatorystrategies.co.uk
www.regulatorystrategies.co.uk