SQUIRE SANDERS

Information Commissioner Publishes SME Guide to IT Security

Introduction

June 2012

Since November 2010, the United Kingdom Information Commissioner (IC) has had the power to levy direct fines of up to £500,000 on businesses and other organisations who fail to have in place adequate security measures for any personal data which they hold. Since then, the IC has shown a significant willingness to exercise this power having levied fines totalling more than £1.5 million to date including, in June 2012 alone, fines to three separate organisations of £640,000 in total. These fines can be imposed in addition to those which other business regulators, such as the Financial Services Authority, have the power to levy.

In a bid to encourage compliance, the IC has published this month its first ever Guide to IT security targeted at small and medium-sized enterprises (SMEs). The Guide is useful practical reading as it goes beyond the very high level data protection principles which every business is required to comply with under the Data Protection Act 1998 to actually detail the sort of IT security measures and procedures which the IC expects SMEs to have in place.

The Benefits of Compliance

Personal data is one of the most valuable assets held by many businesses now. Like other valuable assets, personal data can be exploited for commercial gain but also needs to be maintained and protected against loss, theft or damage and used in accordance with any applicable regulatory regimes.

However, the reality is that many businesses still fail to appreciate the real value of personal data and the risks which loss or damage of that data might cause. Barely a week passes without another news report of a laptop containing customer account details being stolen, or obsolete hardware with patient records still stored on it being offered for sale on eBay.

The benefits of compliance are therefore very obvious. Not only will that help avoid the risk of a six-figure fine (something which few businesses could currently afford), it will also avoid any reputational damage which could otherwise result and the more general costs involved in managing the fallout from a data loss or theft incident, which can often be much higher than any fine. On the more positive side, it will also assist with protecting and maximising the value of a key business asset.

Key Recommendations

Key recommendations of the Guide include:

- **Risk Assessment:** businesses are encouraged to carry out an initial and then ongoing assessment of the type of data which they hold and the risks which they face, and then to adopt security measures which are appropriate to those.
- **Layered Security:** a common flaw in the approach of many businesses to data security is to place too much reliance on a limited set of IT measures (such as the fact that portable devices are encrypted) rather than adopting a holistic approach to risk. The Guide

encourages businesses to adopt a layered approach to security which ranges from physical security of premises and segmentation of servers through to staff training and awareness so that should one measure fail, another is available to catch the threat in question.

- **Secure Data on the Move:** a fundamental and ever increasing risk to data security is the ease with which large amounts of data can be taken offsite on portable devices such as laptops, mobile phones and memory sticks, usually by staff for legitimate work purposes but with increasing frequency by individuals looking to misuse that data for criminal ends. The Guide makes a number of recommendations as to how this risk can be mitigated, including by limiting access permissions; monitoring downloads of data; the use of encryption technologies; and the installation of "kill" software which can be used to remotely erase data stored on lost or stolen devices.
- **Keep Systems Up- to-Date:** the nature of cyber threats changes on a daily basis and most firewall and anti-virus software is only ever as good as its most recent update. The Guide makes the obvious yet extremely important recommendation that such protections need to be kept constantly updated if they are to continue to be of value.
- **Take Responsibility for Contractors:** most businesses, regardless of size, outsource some element of IT service provision, store data offsite with outside hosts or otherwise provide third parties with access to their data. These trends are only likely to increase with the advent of cloud computing. However, many businesses fail to appreciate that, under the UK regulatory regime, they will remain directly liable to the IC and individual data subjects for the acts or omissions of any such suppliers. The Guide encourages businesses to take responsibility for outside suppliers by ensuring that written contracts imposing robust data security obligations are entered into (a legal requirement under the Data Protection Act in any event) and that compliance with those is audited.

What to Do in an Emergency

In the event that, despite your best efforts, your business suffers a data loss or theft incident then it is important not to panic and not to fail to act. In assessing whether to impose fines the IC will look not only at the incident in question and the data which has been compromised but also your response to that incident and your general approach to data security.

In addition, managing a data loss incident properly will assist with minimising liability to individual data subjects who may also bring claims against you independently of any action taken by the IC.

Further Information

A full copy of the Guide is available on the IC website.

Our Information Security Services

At Squire Sanders we have supported a number of organisations caught up in major data loss incidents and can offer clients immediate access to an experienced crisis management team able to assist with minimising the legal and reputational fallout of data loss incidents.

We also work with clients on a daily basis to develop and implement compliance programmes to assist with the protection, exploitation and cross-border transfer of their data and to provide training for staff at all levels from boardroom to frontline customer services.

SQUIRE SANDERS

Contact

Delizia Diaz
T: +44 121 222 3383
delizia.diaz@squiresanders.com

Caroline Egan
T: +44 121 222 3386
caroline.egan@squiresanders.com

Francesca Fellowes
T: +44 113 284 7459
francesca.fellowes@squiresanders.com

Paul Jinks
T: +44 113 284 7234
paul.jinks@squiresanders.com

Ann LaFrance
T: +44 20 7655 1752
ann.lafrance@squiresanders.com

Garfield Smith
T: +44 20 7655 1365
garfield.smith@squiresanders.com