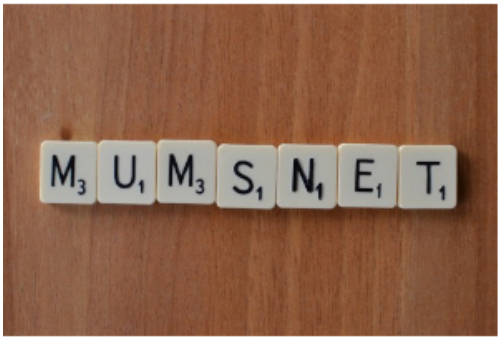
realbusiness

# Mumsnet hacking incident offers lessons for SMEs

11 August 2016 · By Guy Wilmot

**The recent hacking incident involving Mumsnet highlighted the issue of data security for small businesses – and Russell-Cooke's Guy Wilmot shares what SMEs can learn from the event.**




A business can reduce its liability even for a successful hacking attempt or breach

Mumsnet was hacked by a teenager seemingly because it was an easy target. While there are over 200 major cyberattacks reported taking place every month in the UK, the case of the Mumsnet hack was particularly serious as it involved the leaking of user details online.

Many SMEs are in a similar exposed position and could fall victim to a hacking attempt at any time, and must therefore put measures in place to avoid this from happening. It is both a legal and commercial imperative that all businesses be concerned about data and information security.

Legally, any business which holds personal data, which these days means most businesses, is subject to a duty to keep any personal data secure under the Data Protection Act. The Information Commissioner can fine businesses which have not taken sufficient steps to protect personal data which is held by the business. In addition there may be direct liability for negligence or breach of statutory duty to the victims of any successful hacking attempt.

**Read more about securing data:**

- What does Brexit mean for the EU data protection laws?
- Security of personal data: Are you complying with your obligations?
- Four EU business laws that have a dubious future after Brexit

Quite apart from any legal duties being subject to a successful hacking, it can also be extremely detrimental to a company's reputation. Building up a good reputation can take a long time to achieve and a very short time destroy, and can further be very costly to rectify.

Some of the practical steps which can be taken to ensure information security are straightforward.

The first step which many business should take is to ensure that they have invested in the best possible IT security. Putting in place firewalls and other IT security measures is the minimum step which businesses should take to prevent hacking. This is not a technical article but advice should be taken from technical specialists.

However having good or even best-in-class firewalls and IT security can be undermined by human error. Sophisticated technology may be useless if a member of staff discloses key passwords or other security information or does not take adequate steps to put in place a strong password or update it regularly. Some systems can assist in this process by forcing staff to change their passwords regularly and use strong passwords for instance but these are of only limited use.

For this reason it is sensible to put in place a robust IT security policy for employees and staff. The police should deal with password security, remote access to IT systems, the use of staff's own devices and the use of removable media such as CDs and memory sticks.

As well as putting the policies in place it is sensible to ensure that staff have read the policies and are appropriately trained in IT and cyber security.

Clearly the best reason to take these steps is to avoid a successful hacking attempt or breach. A business can reduce its liability even for a successful hacking attempt or breach, if that business has taken all reasonable steps to reduce the risk or the consequences of a breach.

*Guy Wilmot is a partner at Russell-Cooke.*

**Guy Wilmot**
Partner
+44 (0)20 8394 6531
Guy.Wilmot@russell-cooke.co.uk