

Cyber security: What employers need to know

These days many businesses' most valuable assets are not physical but intangible. Closely guarding your confidential information, know-how and intellectual property is vital but what can a business do to tackle the very 21st century problem of cyber security threats?

Intellectual property

The reality is that the most comprehensive, expensive, all-bells-and-whistles online security is going to struggle to prevent someone from using your IP in breach of your rights.

Once you put copyrighted materials and your branding into the public domain, you will be susceptible to people plagiarising your work and piggybacking on your name and reputation. Cyber security systems are not going to help you here but you need to help yourself by registering a trademark and putting a copyright notice on all relevant materials.

Others may still abuse your IP but these simple steps should make it easier for you to enforce your rights when necessary. It is worth noting that taking action against infringers has been made more straightforward and less costly recently with the introduction of a small claims track of the Patents County Court. Also, if someone abuses your IP with a mischievous domain name then you can usually take steps to remove them the domain without having to go to Court.

Confidential information

If someone breaches your security to extract documents, then any use of those documents is likely to amount to a breach of confidentiality. You may want to mark any particularly sensitive information as confidential but by the time someone has circumvented the barriers you have erected and the information is out there, then the damage may have already had been done.

Although it is difficult to completely guard against your confidential information being misused you need to be prepared to act quickly and seek an injunction where the leak could seriously undermine your business.

Data protection

From a legal perspective, decent cyber security may be most valuable in relation to your data protection duties and in fact may be a legal requirement.

As a business in possession of personal information about your clients and customers, you will be expected to have in place adequate security measures to guard against that information being misused.

If personal information in your possession does leak out, then you may receive a stern letter from the Information Commissioner and ultimately be landed with a fine. You will also have a whole host of disgruntled clients and customers. You need to be fully aware of your data protection duties and if you are handling particularly sensitive personal information, you need to consider whether or not this justifies more thorough security measures.

Your cyber security measures need to be proportionate and relevant to the information your business holds and values. But you must also recognise that in many cases your security will not

protect you and you need to be proactive and be prepared to enforce your rights in connection with IP and confidential information when necessary.

Simon Ewing is a solicitor in the corporate & commercial team at Russell-Cooke.

www.russell-cooke.co.uk