Proud winners of 'Law Firm of the Year' at Halsbury's Legal Awards 2015

Employment Knowledge Hub summary sheet

Cyber threats and social media: Protecting your business

30 March 2016

Session summary

This session concentrated on creating a culture of protection for businesses by being proactive rather than reactive in relation to cyber threats and social media issues.

People Management
January 2015

"76% of security threats originate internally."

Cyber threats

- The easiest way to report fraud and cybercrime is via the National Fraud & Cyber Crime Reporting Centre on 0300 123 2040 or online via the ActionFraud website.
- Basic IT security provides a good level of initial protection but cyber security is as much about corporate governance as up to date IT security.
- Reports suggest that 50% of cyber security breaches result from employee error; training and employee awareness is therefore essential.
- It is important to have up to date policies and procedures, including appropriate use of portable devices and home working.
- Specific cyber insurance policies are available and can include not only direct costs but also losses arising from business interruption and damage to reputation.

Social media

- Review and update your current social media policy. If you do not have one, introduce one as soon as possible.
- Such a policy should at least:
  - Clearly set out the rules on what is acceptable during working time and outside of it;
  - Make clear what potential disciplinary action results from a breach;
  - Make clear the potential implications for the business of inappropriate use such as damage to reputation, and;
  - Be communicated to the staff.
- For individual roles it may be appropriate to introduce contractual provisions providing sufficient protection for your business.
- It is important to ensure that not only do you have an appropriate policy but also that employees are aware of and trained in your policies and procedures.
- Each potential disciplinary issue should be treated on its own facts and the usual tests of fairness and reasonableness will be applied by a Tribunal.

Key points to take away

1. Review and update employment contracts to reflect your particular business risks and to provide protection as far as possible.
2. Ensure that you have an incident management plan as part of your risk management process and that this is communicated to all staff.
3. Check what protection your suppliers and/or customers may have as they could be the cause of an attack.
4. Provide employee education and awareness around cyber risks and social media issues, making clear how this could affect them and your business.
5. Create a culture where all employees take responsibility to protect the business, from the Boardroom to the new entrants.

Brachers and Kent HR offer fixed cost services including contract reviews and initial meetings and access to template documents.

Please contact Louise Brenlund on 01622 776405 or Veronica Fox on 01622 655294 if you wold like to discuss how we can help.

Brachers
With you all the way

Call us on **01622 690691** • Visit us at **brachers.co.uk**
Find us on Twitter **@brachers_emplaw** and on LinkedIn **Brachers LLP**