Certainty over regular attendance

Tom Tabori is a barrister at 39 Essex Chambers
@tomtabori
www.39essex.com

On 6 April 2017, the Supreme Court handed down its landmark judgment in *Isle of Wight Council v Platt* [2017] UKSC 28. This appeal arose from the local authority's prosecution of a parent who had taken his child out of school to go on holiday during term time, despite the head teacher refusing permission.

The appeal turned on the meaning of 'regularly' in section 444 of the Education Act 1996. A parent whose child fails to attend school regularly is guilty of a summary offence, and can be prosecuted unless they pay a penalty notice. Proceedings had reached the Supreme Court because the magistrates' court and Divisional Court had held that 'regularly' merely means 'sufficiently often', such that high attendance across the year would be a relevant consideration.

Lady Hale, giving the sole judgment, rejected this interpretation for the following reasons:

- 'Sufficiently often' was far too uncertain to found a criminal offence;
- Crucially, 'sufficiently often' was contrary to the parliamentary intent behind the Education Act 1944 (the 'Rab Butler Act'), the source of the modern law on school attendance, which had introduced a stricter approach; and
- There were good policy reasons why the 'sufficiently frequently' interpretation was unsustainable. Besides clear statistical links between school attendance and educational achievement, unauthorised absences disrupt the education of the individual child and their peers. Worse still, if one pupil can be taken out whenever it suits the parent, then so can others, 'thus increasing the disruptive effect exponentially'.

Lady Hale dealt with the Divisional Court's concern that a single unauthorised absence could lead to criminal liability as follows:

- There are many examples where a minor or trivial breach of the law can lead to criminal liability;
- The possibility of harsh results had not been thought an objection under the pre-1944 law, before parliament had made the law on attendance stricter; and
- Under section 444(3)(a) and (9), a child is required to attend in accordance with the normal rules laid down by the school authorities for attendance but the school

Cyber crime attacks reputations as well as systems

Gus Sellitto is managing director of Byfield Consultancy
@Byfield_PR
www.byfieldconsultancy.com

Ask any in-house PR what they see as the biggest reputational threat for their law firm and the risk of a cyber attack is likely to feature high up on their list. Indeed, the very words 'cyber attack' are enough to induce fear into any custodian of a law firm's reputation. And that fear seems to be increasingly validated by data which shows such attacks are on the rise.

This year's Natwest Legal Benchmarking survey generated a few more column inches than usual because of its findings on cyber crime. It shows that one in four of 269 law firms have fallen victim to cyber attacks. Larger firms have been most affected, with 36 per cent of London outfits having suffered at the hands of cyber criminals. PwC's 2016 Law Firms Survey reported that 73 of the top 100 firms experienced an attack during the last financial year, up from 62 in 2014/15.

The fact that law firms hold valuable data about high-profile organisations and individuals – as well as large sums of client monies – makes them an obvious target. This hasn't escaped the attention of both the Information Commissioner's Office and the Solicitors Regulation Authority. Moreover, from May next year, when the EU's General Data Protection Regulation is enforced, all businesses handling EU citizens' personal data will have just 72 hours to notify data subjects of a breach. This means we are likely to see more data protection breaches being played out in public, with the added risk this type of exposure poses to law firms' reputations.

Apart from the usual risk and compliance procedures firms invest in to try to prevent and plan for cyber attacks, they also need to think carefully about how they communicate in the wake of an attack or a data breach. Here are some of the steps we advise firms to undertake when devising reputation management plans around cyber risks:

- Create communications protocols detailing how you respond in the wake of a cyber attack. They should include internal and external communications with identified spokespeople and a chain of command for escalating enquiries, together with scripts for reception staff;
- Map out the various scenarios that could play out in the event of an attack and, in turn, how each scenario could impact your stakeholders (e.g. staff, clients, the media). Prepare a Q&A document which rehearses and responds to the questions each group might ask you;
- Prepare reactive media and client statements to have ready to distribute, if the