

Third party liability for cyber crime

WHILE IT MAY SEEM OBVIOUS THAT THE perpetrators of crime should be held responsible for their actions, the world of cyber crime opens up responsibility to other parties who may become liable through no fault of their own.

Internet Service Providers (ISPs) may find they are liable for defamatory statements sent through their systems, employers may be liable for the actions of malicious or negligent employees, and cyber criminals may hack into a system and threaten a company's compliance with the Data Protection Act 1998 (the Act). The dangers are there, and to reduce the potential for liability a company must be aware of the risks, monitor the relevant systems and have adequate response protocols in place.

ISPS

For some time, ISPs have been held responsible, to a certain degree, for the content of websites made available through them. The first case of its kind in the UK was as a result of an article posted online more than ten years ago.

The case was *Godfrey v Demon Internet Ltd*. The defendant was an ISP. Part of the service it offered enabled authors to submit articles to the Usenet news server based at their local service provider, which then circulated the postings via the internet.

An unknown individual posted an article, purporting to be by Professor Godfrey, the claimant, which contained defamatory comments about him. The posting occurred on 13 January 1997. On 17 January 1997, Professor Godfrey informed the defendant that the article was a forgery and requested that it be removed. The defendant failed to comply with the request and the article remained posted until 27 January 1997.

The defendant relied on s1 of the Defamation Act 1996, which provides a defence where:

- a) the defendant is not the author, editor or publisher of the statement complained of;

- b) the defendant took reasonable care in relation to its publication; and

- c) the defendant did not know, and did not have reason to believe that what they did caused or contributed to the publication of a defamatory statement.

The Court held that the transmission of a defamatory posting from the storage of a news server constituted a publication of that posting, and that the defendant had been made aware of the defamatory nature of the posting and yet had failed to remove it. The claimant was awarded £15,000 and a costs award was made against the defendant.

This important case cemented liability with the ISP and is an illustration of how inaction can result in liability to the same extent as if a company carried out the offending action itself.

SYSTEM FAILURE

The American retailer TJX, which owns the UK outlet TKMaxx, hit the headlines last month. The company's computer system was subject to a hacking attack, and the credit card details of at least 45.7 million payment cards, used by customers in America, the UK and Ireland, were stolen.

A spokesperson from the Association for Payment Clearing Services (APACS) suggested that any customers who discovered they had been a victim of fraud as a result of the theft would be refunded by their banks.

However, the Information Commissioner's Office has begun an investigation into the company's security procedures. Should it emerge that the theft was a result of lax security standards in the computer system of TJX, the company may find that the banks hold it responsible for any losses, and it could be liable for an unlimited fine.

TJX's position as a victim in this case may be somewhat undermined for three reasons.

First, its system was breached in 2003 when 100 files were moved from its UK computer system. If sufficient improvements were not made to its security as a result of that breach, liability will almost certainly begin to shift in its direction.

Secondly, two further files were later stolen from TJX's system, and the company has admitted that it does not know what they contained. A spokesperson for the company told the BBC (30 March 2007): 'We don't know what was in those files – the technology the hacker used prevents TJX >

'Courts do not look favourably upon companies whose systems are breached because of poor controls.'

Anthony Riem, partner, PCB Litigation LLP
E-mail: ajr@pcbllitigation.com



from knowing, and also the fact that TJX system routinely deletes files.' Although the deletion of obsolete or redundant files should be part of routine file management within a company, it is worrying that the company is unable to identify which files have been deleted and ascertain the content of those that remain.

Thirdly, and perhaps most importantly, the fraud went undetected for 16 months, from July 2005. This suggests a potentially serious flaw in the company's monitoring system.

VICARIOUS LIABILITY

As is often the case, it is not only external threats that must be tackled. A company's liability for cyber crime perpetrated via its computer system is more likely to be as a result of the actions of those working within the company itself, whether through negligence or malice. KPMG reported in January 2007 that 40% of fraud was carried out by company managers who, on average, carried out frauds worth nine times the value of the frauds committed by the people they supervised.

Courts do not look favourably upon companies whose systems are breached because of poor controls or outdated security software. Company directors, who may be held personally liable, must not see this simply as an IT issue. Adequate measures to ensure cyber security should be at the heart of a company's risk management procedure.

Plcs should comply with both the Combined Code on Corporate Governance and the Turnbull Guidelines. These provide a standard for good corporate governance for all companies. Both the Code and the Guidelines stipulate that the board of directors should maintain a sound system of internal control to safeguard shareholders' investment and the company's assets, and the Guidelines suggest the proper ways of doing so. The Code advises that directors should also conduct an annual review and report back to shareholders on all controls including risk management.

Not only do these requirements make good sense in terms of reducing the risks of becoming a victim of cyber crime, compliance will also go a long way as a defence to being held liable for the actions of others.

In June 2006 it was widely reported that a laptop containing information about 243,000 Hotel.com customers, including names and credit card details, was stolen from the car of an Ernst & Young employee. While the theft itself is nothing more than an unfortunate sign of the times, it was only at that stage that Ernst & Young realised that, although the

data was password protected, it was not encrypted. The company later changed its policy: all of its computers now come with encryption software and all password and sensitive information is encrypted. In the event, no Hotel.com customers appear to have suffered any financial loss or identity theft as a result of this incident, although Ernst & Young was certainly exposed to liability for any such loss.

Companies are also responsible for the content of company e-mails and websites. Liability rests with whoever publishes the website, the result being that even if what is posted on the site is put there by hackers, or a negligent or malicious employee, the company is liable.

Risks are reduced by the maintenance of a sound system of internal controls. These should include the identification of areas of the network that are vulnerable to attack, externally or internally. It is important too, that reporting systems are in place to ensure that if the system is breached, the breach is identified and damage limited in a timely fashion.

LIABILITY UNDER THE DATA PROTECTION ACT 1998

The Act requires appropriate technical and organisational measures to be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Where it is proved that a company committed an offence with the consent or connivance or due to any neglect on the part of the officer concerned, that person will be guilty of the offence as well as the company and will be liable to proceedings and punished accordingly.

It is important to emphasise that personal liability may arise through breach of the provisions of the Act through negligence. This could include inadequate protection of data on a company's computer system through out-of-date software or inadequate reporting procedures.

CONCLUSION

Companies should take a proactive approach to cyber crime prevention – complacency is not an option. The keywords are: awareness, monitoring and response.

Computer protection software quickly becomes obsolete, as do the methods used by cyber criminals. Protocols should be updated regularly and employees must be made aware of them to ensure they are implemented effectively. Employees should also be clear on what constitutes confidential information, how it should be stored and with whom

CYBER CRIME PCB Litigation LLP

it may be shared. This is as much for the protection of the directors as for the company itself.

A company should make certain that its website is monitored to ensure that misleading, libellous and offensive material has not been posted by others and, if it has, to have it removed without delay.

Employees' e-mails may need monitoring and the type of information that employees have access to should be examined regularly.

Finally, if the worst does happen, a swift and well-organised response should be taken to mitigate not only loss, but also the extent of any potential liability.

By Anthony Riem, partner, international fraud and commercial litigation, PCB Litigation.

E-mail: ajr@pcbllitigation.com.

Tel: +44 (0)20 7831 2691.

www.pbcclitigation.com.

*Godfrey v Demon Internet Ltd
[2001] QB 201*