The Sony hack: what it means for your company

Date : January 5, 2015

"There are two kinds of big companies in the United States. There are those who've been hacked…and those who don't know they've been hacked" FBI Director James Comey said recently. The Sony pictures hack is possibly the highest profile hack in history. It is a giant in the entertainment industry. Yet in the information age not even the giants are immune to hackers. Whilst full details of the attack are still not known a group calling itself the "Guardians of Peace" claimed that they were behind the hack to Sony's network.

The hack has resulted in :

- the private emails of executives and actors such as George Clooney being leaked;
- trade secrets and marketing strategies going into the public domain;
- movies being leaked before their release date; and
- huge and potentially irreversible brand damage.

Sony decided not to release the film "The Interview" after they received threats apparently originating from a group concerned about the portrayal of the Supreme Leader of North Korea, Kim Jong-un. President Obama said that Sony had made a mistake by deciding not to proceed with the release. Sony then opted to release the film.

This unprecedented tale is a reminder of the power of the hackers. The emails of Sony executives are apparently now in the hands of the hackers. Aside from the reputational and commercial concerns if a company is the victim of a hack it can also find itself in trouble with the law. If your systems are hacked and the information you hold concerning your customers or clients goes into the public domain then your company could be in breach of the Data Protection Act 1998 (DPA 1998). The law says that companies must take "*appropriate technical and organisational measures*" against "*unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."*

Organisational measures mean that employees need to be trained in the DPA 1998. They should also be trained on how to keep client and customer data secure. Companies must also make sure there is appropriate IT security in place including encryption, passwords and virus protection software. Software should also be in place to prevent large amounts of data leaving the network. Enforcement action against a company which has had a hack often includes obliging a company to put data loss prevention (DLP) software in place. Whilst again we do not know the full details yet, if a former employee was involved in this attack, DLP software may have prevented the leak or at least given the company early warning.

In the case of a security breach involving personal data, the UK privacy regulator, the Information Commissioner's Office (ICO) currently has the power to fine a company up to £500,000 for breach of the DPA 1998. The level of fines could increase to 2% of global annual turnover should new EU changes come into force – a possible fine of £99 million in Sony's case. Under the current regime Sony Computer Entertainment Europe were fined £250,000 by the ICO in 2013 when they lost customer data after their systems were hacked.

This monetary penalty followed the Sony PlayStation hack in 2011. The ICO's 2013 investigation found that the attack could have been prevented if Sony's software had been up-to-date, while technical developments also meant that passwords were not secure. The monetary penalty notice issued by the ICO said that Sony should have been on notice to improve their procedures given that they had previously been a target.

The Sony hack shows how important it is to comply with the data protection laws both for your company's profits and its reputation. Cordery provide a range of training on the data protection and data security issues and also advice on crisis management in the event of a data breach. There are more details here and here.

Patrick O'Kane is Compliance Counsel with Cordery in London

Patrick O'Kane, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH

Office: +44 (0)207 118 2700