LEWIS SILKIN

The Perils of Poor Security

James Gill and Bryony Long look at the ICO's recent fining of Carphone Warehouse, and some of the practical steps you can take to help prevent a similar experience.

What happened?

The Information Commissioner's Office (ICO) recently issued Carphone Warehouse with a £400,000 fine following the occurrence of a third party cyberattack in 2015.

The cyberattack targeted a specific Dixons Carphone computer system which hosted internal and external websites, including e-commerce sites. The attackers used valid login details to access the system using out of date WordPress software. At the time of the attack, the computer system in question contained records of over 3 million customers of a number of mobile phone providers (the records included their name, date of birth, marital status and address), as well as historic transaction data covering over 18,000 payment cards and personal records of Carphone Warehouse's employees.

As soon as Carphone Warehouse became aware of the attack, it took steps to secure its systems and notified the ICO, as well as those potentially affected by the breach. However the attack highlighted a number of deficiencies in Carphone Warehouse's security measures which the ICO concluded "played an essential causal role" in the incident. As a result, the ICO found that Carphone Warehouse had seriously contravened the Seventh Principle in the Data Protection Act 1998 (DPA) which states that "appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data" and issued one of its largest ever fines.

What can be learned from this?

Although the ICO acknowledged that there were a number of mitigating factors including the fact that Carphone Warehouse: a) had a programme in place to improve its security; b) took a number of remedial actions to fix the issue and assist the affected data subjects; and c) proactively reported the attack and provided full co-operation with the ICO, these mitigating factors did not stop the ICO from issuing one of its highest ever fines - this just demonstrates how serious an issue poor security is for the ICO. The Seventh Principle is reflected in the General Data Protection Regulation (see Article 32) and is more detailed than under the DPA – this, coupled with the increased fines under the GDPR means that security should always be a high priority both on the Board agenda and in all GDPR implementation programmes, with adequate planning, budget and resourcing to match.

Practical steps

When it comes to compliance with the security principle under the DPA or going forwards under the GDPR, there is no one size fits all approach. Although some sectors may have generally accepted security standards (e.g. compliance with ISO 27001), organisations must assess their own security measures on a case by case basis taking into account the nature of the data processing and the harm that might result if that data is accidentally or deliberately compromised, in each case having regard to technological developments and the costs of introducing new security measures.

That said, there are some helpful reminders from this ruling:

- Regularly implement patches and other remedial steps
- Ensure all software systems are regularly updated and maintained
- Implement a process of verifying that remedial steps have been properly implemented
- Regularly review access controls
- Implement robust vulnerability and penetration testing processes
- Implement appropriate firewalls to monitor and filter traffic from web apps
- Install up to date antivirus software
- Implement attack detection measures and procedures
- Avoid sharing (root and other) passwords
- Know your IT structure
- Ensure data is properly encrypted
- Ensure your data records are regularly cleansed

In addition to ensuring that appropriate technical measures are taken, businesses should take appropriate organisational measures to achieve compliance with the security principle. Such organisational measures may include:

- Identifying individuals or teams who will be responsible for data security
- Training staff to ensure that they are aware of the importance of data security and of your security and use policies
- Putting in place a data breach procedure (including a recovery plan and setting out any notification obligations)

For further information, please get in touch with:

James Gill
Partner, Head of Commercial and Technology

+44 (0) 20 7074 8217
james.gill@lewissilkin.com

Bryony Long
Senior Associate

+44 (0) 20 7074 8435
bryony.long@lewissilkin.com

Francesca Mack
Trainee

+44 (0) 20 7074 8457
francesca.mack@lewissilkin.com

Find out more

twitter.com/LewisSilkin
linkedin.com/company/lewis-silkin