

Press Release

Strictly embargoed until 00.01 on Wednesday 11 November

Burglary and theft account for a third of data security breaches

Fines for reckless data breaches will focus minds at Board level to improve security

New figures from the Information Commissioner's Office (ICO) reveal that burglaries and theft are the single biggest security risks for organisations processing people's personal details. 711 organisations across the public, private and third sectors have reported security breaches to the ICO since 25 million child benefit records went missing two years ago this month; 231 of these involved theft. Several organisations have signed formal Undertakings to step up security at premises to ensure that people's personal details are adequately protected. Over 200 private sector firms have reported breaches to the ICO and 209 NHS bodies, which tend to hold some of the most sensitive personal data such as health records, have identified breaches.

Speaking to data protection chiefs today, David Smith, Deputy Information Commissioner, will say: "Since November 2007 we have taken action against 54 organisations for the most reckless breaches in line with our commitment to proportionate regulation. Some of these breaches would trigger a significant fine for organisations were they to occur after the introduction of monetary penalties in 2010. We are keen to encourage organisations to achieve better data protection compliance and we expect that the prospect of a significant fine for reckless or deliberate data breaches will focus minds at Board level."

The ICO has used the strongest powers currently available, serving organisations with Enforcement Notices and getting chief executives to sign formal Undertakings pledging future security improvements. New powers scheduled to come into force in 2010 will enable the ICO to impose substantial monetary penalties on organisations where there is evidence of a reckless or deliberate data protection breach. The

Ministry of Justice is currently deciding the amounts that can be levied. The ICO is also increasing its auditing role to ensure greater compliance with the Data Protection Act and new powers contained in the Coroners and Justice Bill would give the ICO formal inspection powers across government.

David Smith will continue: “The majority of organisations get data protection right, but regrettably a significant minority of management teams are failing to take data protection seriously enough. Unacceptable amounts of data are being stolen, lost in transit or mislaid by staff. Far too much personal data is still being unnecessarily downloaded from secure servers on to unencrypted laptops, USB sticks, and other portable media.”

Mick Gorrill, the Assistant Commissioner with responsibility for investigations, said: “People’s data has a value. If you had £10,000 you are unlikely to leave it in the boot of your car; you would put it in a safe or deposit it with a bank. In the same way, people’s national insurance numbers, health records and bank details are valuable assets and organisations must take adequate steps to protect personal data. We have investigated organisations, including several NHS bodies, that have failed to adequately secure their premises and hardware, which has left people’s personal details at risk. I encourage organisations, especially NHS bodies, to ensure that the level of security at premises is commensurate with the type of data they are holding. Many breaches are avoidable and are often the result of poor management processes.”

The action that the ICO has taken is listed here:

http://www.ico.gov.uk/what_we_cover/data_protection/enforcement.aspx

Tips on data security are here:

http://www.ico.gov.uk/for_organisations/topic_specific_guides/Data%20security%20tips.aspx

ENDS

If you need more information, please contact the ICO press office on 020 7025 7580 or visit the website at: www.ico.gov.uk

Notes to Editors

1. David Smith is speaking at the annual conference of the National Association of Data Protection Officers.
2. Provisions introduced in the 2008 Criminal Justice and Immigration Act will enable the ICO to impose substantial fines on organisations where there is evidence of reckless or deliberate data protection breaches. The ICO is working with the Ministry of Justice to ensure that we can make use of this power as soon as possible but do not expect this to be until early 2010. The ICO is preparing draft guidance on the use of monetary penalties. The law requires that before the Information Commissioner exercises his discretionary power to impose a monetary penalty – he has to be satisfied that:
 - a. There has been a serious contravention of S4(4) by the data controller,
 - b. The contravention likely to cause substantial damage or substantial distress,
 - c. The contravention was deliberate or
 - d. The data controller knew or ought to have known that there was a risk that the contravention would occur and that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but failed to take reasonable steps to prevent the contravention.
3. The Information Commissioner's Office upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
4. The ICO has specific responsibilities set out in the Data Protection Act 1998, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003
5. Organisations can now sign the Personal Information Promise to demonstrate their commitment to protecting people's personal information by visiting the website at www.ico.gov.uk
6. For more information about the Information Commissioner's Office subscribe to our e-newsletter at www.ico.gov.uk
7. Anyone who processes personal information must comply with eight principles, which make sure that personal information is:
 - Fairly and lawfully processed
 - Processed for limited purposes
 - Adequate, relevant and not excessive
 - Accurate and up to date
 - Not kept for longer than is necessary
 - Processed in line with your rights
 - Secure
 - Not transferred to other countries without adequate protection