

Dealing with toxic data

A privacy impact assessment could help your organisation to manage the risk of a data scandal, as Neil Hodge reports



HIGH-PROFILE personal data losses have prompted the UK's privacy watchdog

to mount investigations into why such errors continue to take place. The Data Protection Act has been around for almost a decade, so why aren't organisations doing better? The regulator wants to know. With so many government departments at the centre of such failures, this has become a hot political issue. Civil servants have been told to perform regular reviews of how personal data is used, protected, and potentially put at risk. This is an area where internal audit can help.

The Information Commissioner Richard Thomas, head of the government's privacy watchdog, says that the proliferation of ever-larger centralised databases is increasing the risk of people's personal data being lost or abused. "It is time for the penny to drop," he said recently. "The more databases that are set up and the more information exchanged from one place to another, the greater the risk of something going wrong. The more you centralise data collection, the greater the risk of multiple records

going missing or wrong decisions about real people being made."

The warning comes as reported data losses have soared in the past year. The number of data breaches – including lost laptops and memory sticks containing sensitive personal records – reported to the information commissioner has risen to 277 since the loss of 25 million child benefit records was disclosed nearly a year ago. Of that number, 80 were reported by the private sector, 75 within the NHS and other health bodies, 28 reported by central government, 26 by local authorities and 47 by the rest of the public sector. The commissioner has launched investigations into 30 of the most serious cases.

"It is alarming that despite high-profile data losses, the threat of enforcement action, a plethora of reports

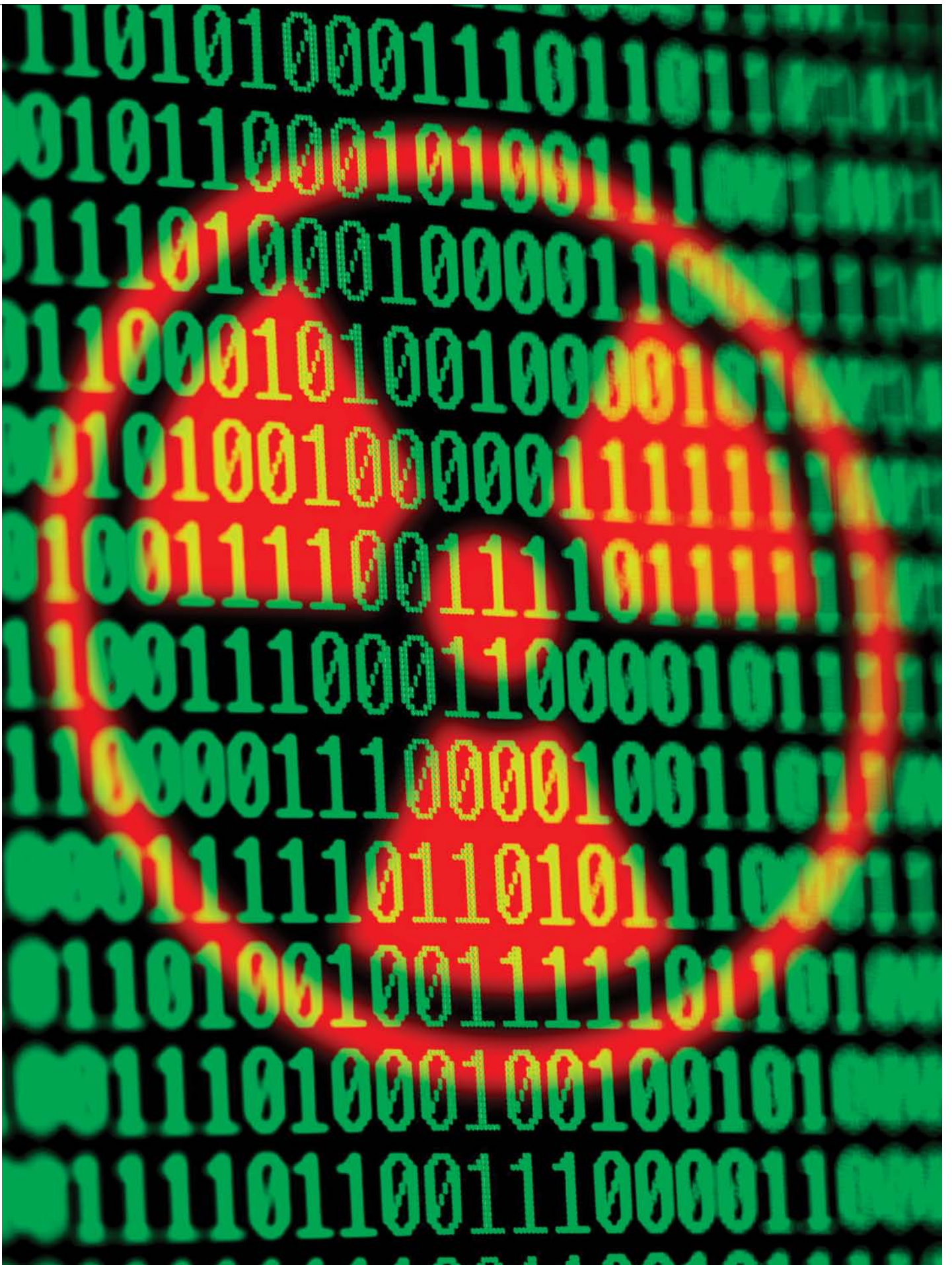
on data handling and clear information commission guidance, the flow of data breaches and sloppy information handling continues," Thomas said.

Breach risk

The Information Commissioner says that data losses have already led to fake credit card transactions, put witnesses at risk of physical harm or intimidation, offenders at risk from vigilantes, falsified land registry records and mortgage fraud.

Thomas acknowledged that the rise in the number of breaches reported to him might be because of improved checks and audits – a welcome result of organisations taking data security more seriously. But he added: "the number of breaches notified to us must still be well short of the total. How many PCs and laptops are junked with »

"Organisations should regard personal data as nuclear material. You keep as little personal data as possible, for as short as possible, and you keep it as safe as possible until the time comes to get rid of it as thoroughly as possible"



“The simplest way to make a privacy impact assessment go as easy as possible is to have a policy embedded throughout the organisation which states categorically that personal data should not be held longer than is useful”

» live data? How many staff do not tell their managers when they have lost a memory stick, laptop or disk?”

To try and minimise further instances of data loss, the Cabinet Office has required all central government departments to carry out a Privacy Impact Assessment (PIA) for any new project started after 1 July 2008. This is a process whereby a project’s potential privacy issues and risks – such as employee and customer personal details, data storage, data access, and IT security – are identified and examined from the perspectives of all stakeholders, and a review is undertaken

for ways to avoid or minimise privacy concerns. The process can involve collecting new data, innovative use of existing data, or providing access to a data set. Because projects vary so widely, these assessments are designed to be flexible so that they can be applied to almost any project.

PIA planning

The information commission says that a well planned and efficiently managed PIA will deliver real benefits to an organisation – in the public or private sector. These include avoiding enforced remedial action after a project’s

launch; retaining public confidence and trust; avoiding potential project collapse; and ensuring that technical and security implications are considered at the right stage of project planning.

However, in guidance that it published in 2007, the information commission says that “a privacy impact assessment needs to be distinguished from a privacy audit.” The commission says that an audit is undertaken on a project that has already been implemented, and that its value lies in the fact that it either confirms that privacy undertakings and/or privacy law are being complied with, or highlights problems that need to be addressed. A PIA, on the other hand, aims to prevent problems arising before the project is even started, so as to avoid subsequent expense and disruption. Hence, a PIA should be carried out in a project’s planning stages – not while it is being implemented.

But the initiative is not without

Your Institute wants you!



Institute of Internal Auditors
UK AND IRELAND

Are you eager to influence the development of the profession? Do you yearn to see the Institute commenting on hot topics in internal auditing? Are you ready to contribute to the running of your Institute?

Then here is your opportunity.

Volunteer for the Institute’s Professional Development Committee and become part of our team, meeting at least four times a year to debate the key issues facing internal auditors in the UK and Ireland and to influence and recommend the Institute’s public positions. PDC is a standing committee of the Council of the Institute so this is an ideal opportunity for personal development.

Drawn from as wide a range of organisations as possible, committee members must support the aims and objectives of the Institute and have strong knowledge and experience of internal audit. They must be willing and able to put in the time commitment and demonstrate an ability to work in a team and to participate in debate. Experience in developing the profession of internal auditing and knowledge of specialist fields welcome.

Informing. Inspiring. Assuring.

To register your interest please send your curriculum vitae to Jackie Cain at the IIA. For further information **tel** 020 7498 0101 or **email** jackie.cain@iia.org.uk

Closing Date

6 January 2009



its critics. Some organisations have expressed concern that the implementation of a PIA could seriously delay a project's start date and encroach on deadlines. Also, the fact that an organisation's compliance units may have to engage on multiple assessments across the organisation on different projects may stretch resources very thinly.

The information commission says that a privacy impact assessment can be carried out in three ways. Firstly, it can be conceived and conducted as a one-time activity, and, if so, it takes into account the information available about the project at the time, and feeds ideas forward into the design. But the commission warns that such an approach has its drawbacks: for example, it cannot reflect information, often of a more detailed nature, that becomes available at a later stage.

Best approach?

Another option is to conceive and conduct a privacy impact assessment as a stand-alone activity, alongside the project and separate from it. However, again, this can create problems, such as creating distance between the staff conducting the assessment and the project team, and resistance to insights arising from the assessment by designers and other project team members.

However, the most beneficial and cost-effective approach, says the commission, may be to conceive of the assessment as a cyclical process, linked to the project's own life-cycle, and re-visited in each new project phase, particularly in major projects. Each version can then take account of both the more detailed specifications that are currently available for the scheme, and the outcomes of previous phases of the assessment. More specifically, later versions can correspond with the later phases of the project, such as requirements analysis, logical design, physical design, construction, integration and deployment of the new system, or their equivalents in whichever project method the organisation uses.

Eleven steps

The Information Commissioner issued a handbook last year on how to approach carrying out a Privacy Impact Assessment. Below are 11 key questions organisations and internal audit need to ask to help decide if an assessment is necessary. Does the project:

- 1 Apply new or additional information technologies that have substantial potential for privacy intrusion? Examples include smart cards, locator technologies (including mobile phone location, applications of GPS and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining, and logging of electronic traffic.
- 2 Involve new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes?
- 3 Have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?
- 4 Involve multiple organisations, whether they are government agencies (such as those in "joined-up government" initiatives) or private sector organisations (as outsourced service providers or as "business partners")?
- 5 Involve new or significantly changed handling of personal data that is of particular concern to individuals?
- 6 Involve new or significantly changed handling of a considerable amount of personal data about each individual in the database?
- 7 Involve new or significantly changed handling of personal data about a large number of individuals?
- 8 Involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?
- 9 Relate to data processing which is in any way exempt from legislative privacy protections?
- 10 Justification include significant contributions to public security measures?
- 11 Involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?

To download a free copy of the ICO's Privacy Impact Assessment Handbook, go to: http://www.ico.gov.uk/Home/for_organisations/topic_specific_guides/pia_handbook.aspx

Finally, the commission suggests that the organisation may conduct a more general risk assessment as part of the project, or may have generic risk management processes in place. If so, consideration should be given to undertaking the privacy impact assessment within the context of a broader risk management framework.

Steve Wright, senior manager in risk assurance services at PricewaterhouseCoopers (PwC), says: "Carrying out these assessments well >>



Department for Work and Pensions is the biggest data controller in Europe

» really relies on functions like internal audit, IT and compliance being organised enough to get involved at the very beginning of the process, and to try to co-ordinate how those involved in the project identify, report and mitigate other privacy issues that may come to light during the project's life-cycle. Management buy-in is crucial here, otherwise staff will leave the handling of data issues to compliance to detect and deal with, and that shouldn't happen."

Early start

Experts and practitioners agree that a privacy impact assessment should be carried out before a project begins. "Assessments work best on 'green field' projects where data is being newly acquired and you can build controls from scratch," says Simon McDougall, director and head of the privacy and data protection team at Deloitte & Touche. "We have seen the privacy impact assessment methodology struggle when it is used to review legacy data sets and proposed modifications to existing processing where a formulaic approach may not be flexible enough. Privacy impact assessments should be done early in the process and can often be integrated with other impact assessments, hence saving time and resources and avoiding repetition."

Chris Bywater, head of business continuity and security at the Department for Work and Pensions (DWP), the biggest data controller in Europe with 100,000 employees, says that in practical terms, "a privacy impact assessment is no more onerous than a security authentication review, except that it also needs to take account of personal data issues as well."

"What is crucial, however, is the timing of the assessment. It really needs to take place in the planning stages of any project, and not after the project has begun. Central government departments are still finding their feet with regards to how privacy impact assessments can best be carried out and the whole process will take a long time to embed, but we're getting there. Crucially, there needs to be a culture change – not just in central government, but in all organisations – where employees need to guard other people's data as preciously as they do their own. Once that happens, data breaches will be massively reduced," he says.

Peter Livingstone, a partner in intellectual property and IT law at law firm Clarke Willmott, agrees that attitudes towards personal data need to change in order for data management and data protection to work properly. "Organisations should regard personal

data as nuclear material," he says. "You keep as little personal data as possible, for as short as possible, and you keep it as safe as possible until the time comes to get rid of it as thoroughly as possible."

Data retention

Livingstone says that organisations will struggle to carry out privacy impact assessments well if they are unable to get their data retention policies in order. "If some organisations are going to continue to record every car that comes into their car parks, tape every marketing call for 'training purposes' and hold on to that as well as other customer data for five years, then they are putting themselves at unnecessary risk of committing a serious breach of privacy," he says.

"Not only will the cost of storing that amount of data be difficult to maintain and monitor, but it may also compel internal audit and other compliance functions into thinking that they need to allocate greater resources than necessary when they are asked to work on a privacy impact assessment," he adds.

"The simplest way to make a privacy impact assessment go as easy as possible is to already have a policy embedded throughout the organisation which states categorically that personal data should not be held longer than is useful. Once that is done and the 'useless' data scrapped, the process should be a lot easier as everyone in the organisation will be a lot more 'data aware'," says Livingstone. ●

"Carrying out these assessments well really relies on functions like internal audit being organised enough to get involved at the very beginning of the process"