Findings from ICO information risk reviews of incident management at 10 local authorities

February to August 2017

Information Commissioner's Office

Introduction

The Information Commissioner's Office (the ICO) enforces and promotes compliance with the Data Protection Act 1998 (the DPA), which contains eight principles of good information handling. The ICO will maintain an equivalent role in respect of the General Data Protection Regulation (the GDPR), which will take effect in the United Kingdom from 25 May 2018.

In late 2016 there were two information security incidents involving local authorities. The incidents, which were potentially serious, were not reported to the ICO. While the current DPA does not require local authorities to report such incidents, it is good practice to do so. Under the GDPR, it will be compulsory in some high risk cases.

As a result of the breaches, the ICO's Enforcement Department carried out a statistical analysis and found that the number of self-reported breach incidents from local authorities was low compared to the potential for information rights concerns.

Following the analysis, the ICO identified which local authorities were likely to process higher volumes of sensitive personal data and offered them an information risk review.

Ten local authorities agreed to a review. The ICO's Assurance Department conducted the desk-based reviews via telephone with the data protection compliance lead at each authority between February and August 2017.

This report is based on these reviews. It highlights our experience of information security incident management at these local authorities and is intended to help them and others in the sector to recognise where they can make improvements to this area. No individual organisation is named in this report.

What we assessed

When we conducted the reviews, we assessed the controls that the local authorities had in place for information security incident management and the extent to which those arrangements were effective. Where we identified information risks, we have made recommendations to mitigate these and improve assurance against specific controls.

The relevant control areas were:

- incident management policy: existence of a policy providing a framework for reporting and managing information security incidents,

- ownership and understanding of incident management responsibilities: management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents,
- incident reporting and feedback procedures, including reporting to the ICO: staff should be aware of the nature of an information security event, its potential detriment to the organisation and how to report it,
- appropriate escalation of incidents: information security incidents should be responded to in accordance with the documented procedures, and
- incident logs and review of incident management systems: evidence of lessons learned and consideration by senior management.

The examples identified within this report were not always consistent across all of the organisations we spoke to, however they were evidenced in at least one local authority that participated.

Areas of good practice

The reviews identified areas of good practice in information security incident management controls:

- involvement of senior individuals with core data protection and/or information security roles in incident management,
- template forms to report and capture key information about incidents,
- initial risk assessments to establish the severity of incidents;
- record of details of investigations on electronic systems or folders,
- involvement of the Senior Information Risk Owner (SIRO) in determining whether or not reporting to the ICO is appropriate,
- implementation of an Information Security Incident Log,
- discussion of information security incidents at the Corporate Information Governance Group (CIGG), and
- staff awareness of information security incident management policies, procedures or guidance, incidents at their own or other organisations through briefings, emails, the intranet, newsletters and/or team meetings.

Areas for improvement

We made recommendations to help local authorities improve their information security incident management controls:

- develop a process for assessing and grading risk so that all qualifying incidents are reported appropriately to the ICO and any outcome of decisions to report is noted,
- incidents and events should be reported within the appropriate timescales. It is worth noting that the GDPR will introduce a duty on all organisations to report an information security incident which is likely to result in a risk to the rights and freedoms of individuals, to the ICO within 72 hours of becoming aware of it,
- decisions as to whether or not to notify any incidents to the ICO should be noted on incident logs, to facilitate monitoring and trend analysis,
- ensure there are adequate document controls for annual review and compliance monitoring of policies, which include roles and responsibilities and process flowcharts. The content of these policies, procedures and guidance should be tailored to the relevant audience. All employees should be made aware of their existence and they should be easily available,
- policies and procedures should require employees to report manual and electronic information security events and incidents,
- checks and tests (internal audit) should be regularly undertaken to ensure adherence to information security incident policies, procedures and guidance,
- develop content and delivery of information incident security management training as part of mandatory data protection induction training. Training should be refreshed annually,
- introduce training targets, accurate reporting on training completion and regular reporting to senior management. This will be critical to future GDPR proofing,
- ensure individuals with core responsibilities for information security incident management receive specialised training in line with those responsibilities. This will be critical to future GDPR proofing,
- corporate induction checklists should incorporate accurate and specific reference to key information security incident management policies, and also state that it is mandatory for line managers and employees to sign off these checklists to enforce compliance,
- where feasible appropriate contingency measures should be in place so that there is adequate resource to cover any absence of key staff in the event of an information security incident,
- ensure internal audit have visibility of the management of risk incidents to enable periodic management reviews,

- use the logs to identify trends and patterns in risk incidents. This may help in preventing further possible larger incidents from forming. It may be helpful to look at the information security incident trends reported for the local government sector on our website ico.org.uk,
- establish a range of information security incident management key performance indicators (KPIs), report against these on an ongoing basis and ensure that the audience for these reports includes appropriate individuals and teams. Ensure any trends are regularly considered and acted upon,
- it may be helpful to consider alignment with external standards, for example ISO27001, as appropriate, and
- local authorities should share information security incident management good practice with each other at appropriate local and /or national forums to help them and their counterparts in the sector to recognise where they can make improvements.

What else we found

- Five incorporated information security incident management content (at least in regard to reporting) within overarching policies, principally the Information Security Policy, but alternatively the Data Protection or Information Governance Policy in some instances.
- Eight dedicated information security incident management policies, procedures or guidance.
- Six incorporated examples of information security incidents within relevant policies, procedures or guidance.
- One incorporated an information security incident management process flowchart within relevant policies, procedures or guidance.
- Three did not consistently undertake reviews of their information security incident management policies, procedures or guidance on at least an annual basis. The ICO Local Government Information Governance Survey concluded more generally that 43.4% of local authorities subject their information governance policies to annual review.
- Two participating in the information risk reviews did not incorporate adequate document controls in regard to relevant policies, procedures or guidance.
- Two had formal ISO27001 accreditation and 20% seek to align their information security incident management policies, procedures or guidance to ISO27001. It is noted that this figure is significantly lower than the 88.4% of local authorities which confirmed in the

ICO Local Government Information Governance Survey that they align or accredit to ISO27001.

- All have or are in the process of ratifying a template form to report information security incidents. This is good practice.
- Five did not document procedures for determining whether or reporting a breach to the ICO is appropriate. One consulted ICO guidance when considering reporting to the ICO. One reported high risk incidents to the ICO within 72 hours of the risk assessment. Three did not consistently record their decisions as to whether or not to report incidents to the ICO on their incident logs.
- Nine assigned responsibility to the Senior Information Risk Owner (SIRO), alone or in conjunction with others, for determining whether or not notification to the ICO is appropriate.
- All assigned corporate individuals and/or teams with core responsibilities for data protection and information security, to coordinate the reporting, assessment, investigation and/or response to information security incidents.
- Five created a record of each information security incident investigation within either a case management system or restricted folders utilised by corporate individuals and/or teams with core responsibilities for data protection and information security.
- Eight undertook a formal risk assessment to establish the severity of the information security incident; this is good practice. Six used a matrix and/or scoring technique, and a further two utilised the NHS Serious Incidents Reporting Investigation Tool (SIRI). It is important to recognise however, that local authorities should use SIRI in respect of incidents involving health and adult social care personal data. Accordingly, these local authorities should ensure that they have adequate and alternative mechanisms in respect of incidents involving other forms of personal data. Local authorities may find it useful to consider the NHS Digital Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation for further information in regard to SIRI.
- Five included content in regard to information security incidents within their reports to the senior leadership team and/or SIRO, one to the Assistant Directors and two to some Directorate of Management Teams (DMT) s. The frequency of this reporting ranges from monthly to annually. Two local authorities included content in regard to information security incidents in their annual information governance reports.
- Seven had established a Corporate Information Management Group (CIGG) which discusses and/or reviews information security incidents. This is good practice.

- Two did not have information security incident KPIs. It is noted that this figure is significantly lower than the 87.9% that was reported in a wider survey of local government conducted last year which is available here: Local Government Information Governance Survey.
- Nine participating in the information risk reviews have a log. This figure is further corroborated by the ICO Local Government Information Governance Survey.
- One shared good practice in respect of information security incident management with neighbouring local authorities at a regional group.

Further guidance

The ICO has produced guidance for organisations on information security incident management. This information can be found on our website:

- The report a breach page
- Guide to the GDPR personal data breach page