Information Commissioner's Office

Findings from ICO information risk reviews of information security in the higher education sector

April 2017 to March 2018

Introduction

The Information Commissioner's Office (the ICO) enforces and promotes compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA18), which came into force in May 2018.

This report is about information risk reviews that took place before May 2018, so they were assessed in line with the Data Protection Act 1998 (DPA98) and its eight principles of good information handling.

The ICO Enforcement Department publishes quarterly updates of information security incident trends on our website. These updates explain where and how organisations should improve.

Information security incident trends.

The education sector consistently falls within the top five sectors for the number of reported information security (IS) incidents. The third quarter of 2016/17 showed a 40% increase in IS incidents for the sector. We therefore decided to focus this review on IS controls at universities.

How we conducted the reviews

Sixteen universities agreed to participate in the reviews, which took place between April 2017 and March 2018. They were conducted by our Assurance team as both physical visits and telephone conferences, after desk-based reviews of documentary evidence we received. Following the reviews each university was issued with an individual reports highlighting our observations and making recommendations to address any weaknesses that were identified.

What this report does

This report is based on these information risk reviews; it highlights our observations of IS management at these universities and summarises the main trends, areas of good practice and weaknesses. This report is intended to help the higher education sector more generally by assisting other universities to recognise where they could improve and to share good practice. No individual organisation is named in this report.

Control areas

When conducting the information risk reviews, we assessed the controls that the 16 universities applied to IS management and how far these were effective. Where we identified risks, we made recommendations to mitigate them and to improve assurance against specific controls.

The relevant control areas were as follows:

Information Security - Organisation
Establishing a management framework to initiate and control the implementation and operation of IS in the organisation.

Information Security - Policy
Providing management direction and support for IS in line with business requirements and relevant laws and regulations.

Information Security - Training and Awareness
Ensuring that employees and contractors are aware of and fulfil their IS responsibilities.

Information Security - Incident Management
Ensuring a consistent and effective approach to the management of IS incidents, including communication on security events and weaknesses.

Information Security – Compliance and Monitoring
Ensuring that IS is implemented and operated in line with the university's policies and procedures.

Areas of good practice

The following represents some of the good practice we found during the risk reviews. These examples were not consistent across all 16 universities.

- An overarching IS Policy that defines the roles and responsibilities of key IS staff. This is supported by specific policies and procedures including risk and incident management, mobile working and network security. Policies and guidance are made available for staff on internal intranets, with some being accessible on external websites to promote transparency.

- Policies and procedures undergo regular reviews. They are entered on a log or there is a corporate document index, maintained by an appropriate senior member of staff, which lists the approval and future

review dates. Policy owners are then notified when policies are due for review.

- Creating a network of Data Protection (DP)/IS coordinators or champions across all departments, including academic schools, to support the activities of steering groups. The responsibilities of these include developing and disseminating DP guidance, raising awareness of IS issues, risk management and incident reporting. The network meets regularly and escalates issues to appropriate roles and groups.

- Information risk management is detailed in a separate policy along with detailed risk-assessment and escalation procedures. Information risks are recorded on local registers by departments and also on a central information risk register held by the IS team to provide oversight.

- DP and IS training are mandatory for all staff.

- DP/IS training is supplemented with various awareness-raising activities such as regular items in staff newsletters, face-to-face briefings, screensavers, leaflets and blogs. Subjects covered include password guidance, email phishing scams, protection of mobile devices and practical tips when working with personal data.

- DP/IS training is delivered in a bespoke face-to-face format for staff such as cleaners who do not use computers at work and so may not have access to the online courses available to network users.

- Clear guidance, available on internal webpages, informs staff about how to report DP/IS incidents. Accessible reporting methods are in place, along with details of staff responsible for handling the incidents.

- IS incidents and trends are discussed as a standing agenda item at steering groups and escalated to higher-level committees, such as executive boards and audit committees, where appropriate, with involvement from the Senior Information Risk Owner (SIRO).

- Internal and external auditors conduct regular IS audits. Findings are reported to audit committees to ensure all audit actions are implemented within agreed timescales.

- Vulnerability assessments of key information systems are performed regularly. Penetration testing takes place when weaknesses are identified.

- Decommissioned mobile devices are confidentially destroyed by a third-party contractor. Confidential-destruction certificates are provided for every item. Some universities have visited the contractor to audit their

destruction processes, which gives assurance that the contractor is working to best disposal practices.

Detailed findings and areas for improvement

During the reviews, we identified a number of areas of weakness. We made recommendations to help the individual universities tackle these. We outline some of the key recommendations in the blue boxes below, particularly where they address weaknesses identified in several of the universities. Universities that did not take part in our reviews may also wish to consider acting on these recommendations.

Information Security - Organisation

- Only 50% of the universities reported taking steps to prepare for GDPR. In most instances this included creating a GDPR working group or strategy. However, as expected, GDPR preparation was more advanced in the universities involved in the latter stages of the review period.

- Most universities had allocated responsibility for IS at board and operational levels. Several had split responsibility for DP compliance and IS into different teams. Operational responsibility for IS was often allocated to teams responsible for maintaining and securing IT systems. In some instances this responsibility was documented but this was not consistent; job descriptions and policies were not always accurate and updated.

- Most universities were taking steps to create or already had an Information Asset Register (IAR). Some had allocated Information Asset Owners (IAOs) to the identified information assets but others had not completed this. Academic departments were not always included.

Recommendation: Universities should undertake information flow mapping to ensure their IARs are complete and record all personal data held in electronic and physical form. IARs should include data held by academic schools and other departments. IAOs should be allocated and trained. IAO responsibilities should be documented in job descriptions or relevant IS policies (or both). IARs should then be subject to regular documented reviews to ensure they remain accurate, up to date and consistent.

- The GDPR and Data Protection Act 2018 require organisations that are public authorities, or that carry out certain types of processing activities, to appoint a Data Protection Officer (DPO); this includes

universities. At the time of our reviews, this requirement was not in place but 44% had already appointed a DPO and others were taking steps to do so. 50% of the universities had already assigned the role of SIRO, who could be considered for the DPO role.

- All of the universities had senior-level steering groups or committees in place. These provide general oversight for information governance and DP compliance activity.

- Information risk management varied greatly. Some universities had specific policies detailing how to identify, assess, record and escalate information risks. Others incorporated information risks in their general risk-management processes. Risk registers also varied, with some recording information risks on local departmental registers and escalating them to corporate registers where appropriate. We consider that identifying and recording risks locally and then incorporating entries into a corporate information risk register is good practice.

Recommendation: Universities should ensure that information risk-management policies and procedures include physical information risks as well as IT-related risks. Roles and responsibilities should be documented as well as the assessment, grading and escalation processes. Risk registers should record details of the risk, classification, risk owners and progress. Regular reviews should be documented.

- Most of the universities had introduced measures to encourage the completion of a data protection impact assessment (DPIA) for new, or significant changes to, projects and systems. However, none of the universities had a formal policy or procedure to inform staff of when and how to complete DPIAs.

Information Security - Policy

- 75% of the universities had an overarching IS Policy. Several of these were supplemented by specific detailed policies or procedures to give guidance for staff on the security measures that should be in place.

- Most universities had reviewed and updated their DP/IS policies ahead of GDPR, or were doing so, but we saw little evidence of regular reviews having been undertaken in the past.

Recommendation: DP/IS policies and procedures should be reviewed on an annual basis to ensure they are accurate and fit for purpose. They should be version-controlled and formally approved by staff or boards who have the expertise and authority to do so.

- We saw little evidence that universities were taking appropriate steps to ensure that staff had read and understood relevant IS/DP policies and procedures, including subsequent updates.

Recommendation: All permanent, temporary and contract staff should be required to confirm they have read and understood all IS-related policies and procedures.

Information Security - Training and Awareness

- All of the universities provided some DP training for their staff; 75% made completion mandatory and 87.5% provided specific IS training.

- Only 37% of the universities required staff to complete refresher training regularly; 12.5% required training to be completed annually.

Recommendation: The requirement for all staff, including temporary and contract staff, to complete DP/IS training should be mandated to ensure that all staff have been trained in their responsibilities. Such training should be completed regularly. Training content should be regularly reviewed and updated to ensure it is fit for purpose and covers current concerns.

- Only one of the universities ensured that new staff completed IS training as part of their induction before being granted access to systems. Some allowed up to six months.

Recommendation: To ensure that staff are aware of their IS responsibilities when processing personal data, universities should ensure that new starters complete IS training in the first week of employment and before being granted access to systems.

- Only 25% of the universities provided specialist IS training for specialist IS roles. Some were planning to have this in place for GDPR.

Recommendation: Universities should undertake a regular training-needs analysis for all employee groups with personal data handling responsibilities, to ensure that these individuals receive role-specific IS training. In this regard, universities should particularly consider specialist roles such as IAOs, DPOs and SIROs.

- To ensure that the training had been understood, 56% of the universities included a test as part of their DP/IS training package. Not all these tests required staff to achieve a certain pass rate. Others had the pass rate set too low.

Recommendation: DP/IS training programmes should involve a test with a pass rate set high enough to give assurance that staff have understood the content to a sufficient level. To give this assurance, most recommended courses require a pass rate of 80%.

- Only 25% of universities had effective systems in place to monitor training and ensure it had been completed.

Recommendation: Universities should record and monitor the completion of IS training by all staff. Key performance indicators or targets should be agreed and measured against each department and the university as a whole, and discussed regularly at steering-group meetings. To ensure that staff are aware of their responsibilities, non-completion of the training should be followed up.

- We found that most universities did not have regular forums to discuss IS concerns.

Recommendation: Universities should consider introducing regular forums or groups to discuss IS concerns/issues at a local level. These groups should be chaired by an appropriate senior member of staff and include representatives from professional services, departments and schools. Procedures should be in place to escalate issues to the appropriate steering groups. Staff should be aware of the name of their department's representative.

Information Security - Incident Management

- 31% of the universities had specific documented IS incident-management policies or procedures. Others had procedures for responding to IT incidents or cyber incidents but these did not include guidance on responding to physical IS incidents or those involving hard-copy personal data. We saw evidence of IS incident management being included in other information-handling policies and general incident-management processes, which is good practice.

Recommendation: An IS Incident Management Policy or Procedure (ISIMP) should be in place, setting out roles and responsibilities for identifying, reporting and managing electronic and physical IS incidents. The policy should be reviewed annually and communicated to all staff to ensure they are aware of their responsibilities.

- Only 19% of the universities had effective ways of ensuring staff knew how to report IS incidents. Problems included a lack of clarity on

how staff should report incidents and what information they should provide. Often, staff knew little of the incident-reporting process.

Recommendation: Clear and accessible IS incident-reporting methods should be made available to help staff report incidents. Incident reporting should be included in the mandatory IS training for all staff and contractors. Detailed reporting procedures should be formalised. This will help ensure that all IS incidents are effectively reported, logged and managed, and will help prevent further incidents.

- We saw evidence of formal assessment and classification procedures for IS incidents at 19% of the universities. Some had informal assessments by nominated staff such as the SIRO, whereas others identified serious incidents but the relevant criteria and responsibilities were not documented.

Recommendation: Universities should document the requirement to risk-assess and classify IS incidents according to their severity, along with guidance on any required follow-up action. These actions could include compliance with the incident-reporting obligations under GDPR. The incident should be reported to the ICO within 72 hours where there is a resulting risk to people's rights and freedoms. Consideration should also be given to notifying affected data subjects.

- Most universities keep a log of IS incidents but we were concerned that these were not always comprehensive – not all reported electronic and physical incidents involving personal data were being included. Often, responsibility for DP and IS compliance was split across separate departments with separate reporting arrangements. Incident logging was more effective in universities that had a central log or clear communication methods between departments (or both).

Recommendation: A central IS incident log should be in place to record details of all reported electronic and physical IS incidents. The log should include a description of the incident, the name of the individual who reported the breach, the name of the incident handler, details of any actions taken to resolve breach, details of any escalation (internal and external), and any lessons learned. The log should be maintained and updated by staff in key roles to ensure all reported incidents are recorded and resolved. If it is decided not to report a breach to the ICO, this should be documented as it may need to be justified.

- Escalation of IS incidents varied greatly, with only a few universities regularly discussing incidents at appropriate steering groups. Escalation processes worked better at universities that documented their risk-assessment and reporting requirements and specified the responsibilities of roles such as SIRO and DPO.

- We saw little evidence of staff being encouraged to report near misses. Where procedures specified that near misses should be reported there was little evidence that staff were confident enough to do so.

Recommendation: Encouraging staff to report near misses will allow universities to identify, collate and monitor trends which might indicate areas of weakness and risk more effectively. Universities should require staff to report any observed or suspected security weakness in the system or services.

- Often, discussion of lessons learned was informal. Some universities communicated lessons learned to staff or fed them into their training programmes.

Recommendation: Universities should formally document lessons learned from IS incidents. They should have in place ways of enabling the type, volume and cost of IS incidents to be monitored and quantified. The information gained from evaluating incidents should be used to identify recurring or high-impact security incidents. Lessons learned should be communicated to all staff across departments and included in training and policies.

Information Security – Compliance and Monitoring

- All the universities had an internal audit function and 81% had conducted specific IS audits in the last year. However, some could not evidence that they would perform these regularly on an ongoing basis.

Recommendation: IS and other internal audits involving the processing of personal data should be undertaken regularly to identify weaknesses in risk and control processes. Audit plans and schedules should formally document the audits to be carried out. Actions to tackle the risks identified should be documented.

We found that many of the universities did not have clear-desk and clear-screen policies.

Recommendation: Clear-desk and clear-screen policies or procedures should be in place to prevent unauthorised access to personal data. Documents containing personal data should be locked away when not in use and computer screens locked when unattended.

- We observed insecure storage of confidential waste at 12% of the universities. Confidential waste awaiting disposal should be held in a lockable confidential waste console, or in a secure, lockable area.

- To ensure compliance with IS policies and procedures, 12% of the universities had applied spot-checks but these were not taking place regularly.

Recommendation: To ensure compliance with IS policies and procedures, managers across all departments should carry out key system reviews and spot-checks. These should include checks on compliance with clear-desk and clear-screen requirements and the storage/disposal of confidential waste. Results should be reported to the recommended risk-management steering group to ensure central oversight of staff awareness and compliance.

- Most universities conducted vulnerability assessments and penetration testing on their systems. But some reported that they did not regularly test all systems used to process student data.

Recommendation: Regular, routine technical compliance reviews of systems used to process personal data should be carried out. These should include vulnerability assessments and penetration testing. Identified risks should be documented and actioned. To ensure patches are applied in a timely way, patch updates and their management should also be documented.

- There was inconsistency in the use of removable media by staff, particularly regarding USB memory sticks.

Recommendation: To prevent the unauthorised appropriation of personal data and the downloading of unauthorised content onto their networks, universities should consider locking down USB ports and other drives that can be used for removable media. Staff with a legitimate reason could be granted access to certain ports when there is a business need. However, this should only be done using encrypted USB sticks provided by the university.

- Several of the universities had achieved or were planning to achieve Cyber Essentials accreditation, with others aligning their processes and procedures with ISO 27001:13 standards.

Resources

The ICO has produced guidance for organisations to consult in relation to information security. This can be found on our website www.ico.org.uk:

- Guide to GDPR
- Information Security Checklist
- Guidance on personal data breaches
- Notification of data security breaches to the ICO
- Data protection breach notification form.