Information Security Oversight Committee  
Monday, 30th April 2018

Minutes

Present: Richard Bartlett (RB), Carolyn Read (CR), Stephen Jones (SJ), Rich Hutchinson (RH), Nigel Berryman (NB), Peter Gibbin (PG), Guy Williams (GW), Stefan Graf (SG), Jonathan Wilson (JH). Victoria Hollamby (VH) also attended the meeting with CR to represent Information Governance.

Apologies: Lydia Drumright (LD) and Kieran Lovell (KL).

2. Minutes of the Previous Meeting and Matters Arising

The minutes of the meeting held on Friday, 26th May 2017 were approved, and the following matters arising were noted by RB:

a. The induction pack did include reference to information governance training, however RB had contacted the School HR BM to discuss improvements including general context, updated training, reference to policy and UIS published guidance.

b. RB was still not clear about the public facing "http://www.cam.ac.uk/email-and-phone-search", and how this fitted in with GDPR.

AP (1) - RB to flag up the GDPR related email and phone directory issue with KL.

c. More clarity had been provided in breach reporting, but GDPR made this more important as the timeline after a breach was key.

3. Objectives

a. Setting Policy

i. Impact of GDPR. DPA (and IGT) previously drove a lot of information security efforts, GDPR now drove those harder, and placed greater emphasis on accountability, breach reporting, and potentially fines for breach resulting from non-compliance.

ii. Need for better assurance mechanisms cross-School. In view of the lack of dedicated resources, RB suggested this was enabled by requiring involvement from everyone (similar to Health and Safety). RB added that a paper would follow with a proposal, but in theory assurance could be enabled by involvement from Departmental Research and HR administrative staff, Data Managers, PIs, DA/BOMs, HoDs (for sign off only), and all those tied into School Research Office, HR, Information Governance, DA/BOM meeting/General Division, and Heads of Department meetings/Council of School. He said that peer review/auditing would not be possible with current resources, but he asked the Committee whether it would support mandatory/strongly encouraged reporting of assurance to some sort of School level body. This could be tested through spot-check audits. Safe havens would still require explicit review though and this was currently CSCS based.

AP (2) - CR to speak to School HR about leaver procedures.

AP (3) - RB to draft a paper on possible cross School assurance mechanisms and then circulate to the Committee.
iii. **NIH consent forms.** GR said that when consent forms for data were signed, they agreed to follow best practice but there was no enforcement. However he noted that there would be huge ramifications if NIH data was lost.

b. **Reviewing Implementation**

i. **Efficacy of software update management (Windows, Mac and Linux).** RB said that everyone should be able to measure and manage updates for the platforms they were responsible for. He asked the Committee whether there were any challenges they should be aware of. None were reported and no-one was sure who had originally raised this matter.

ii. **Cyber Essentials or Cyber Essentials Plus as a potential assurance level for the School.** This has been suggested by KL previously, it had now been discussed and generally agreed at the Campus IT meeting. The Committee agreed to recommend that Cyber Essentials Plus for all Safe Havens and Cyber Essentials for everyone else would provide an appropriate level of assurance.

   **AP (4) - PG to verify password requirements.**

c. **Review of Safe Havens**

RB noted that two new safe havens were planned (MRC CBU and UIS). These would need to be reviewed, and a report on new safe havens including a recommendation considered by this Committee, and a decision made on whether to approve or request further action prior to approval.

d. **Maintaining Information Governance Toolkit**

RB reported on the New Data Security and Protection Toolkit. This was a departure from the previous toolkit, and was largely (in his opinion) an improvement, but it had not yet been fully considered. Any safe haven should ideally have Cyber Essentials Plus or greater before submission as this would preclude a chunk of the questions. He said that CSCS would happily go first on this and he asked the Committee whether there were any issues with other providers following in its footsteps (e.g. WBIC, MRC Epid and potentially MRC CBU?). No issues were reported.

e. **Review breaches**

RB told the Committee that none were reported at School level. CSCS had one availability issue caused by human error (no breach) and had observed one near miss where someone extracted a ‘backup’ of the data for an entire study to an external hard drive from the SDHS. This was logged as a non-conformity of the ISMS and the data was wiped. He added that the lesson learnt from this incident was that Data Manager awareness of appropriate data handling was key.

   **AP(5) - RB to discuss Data Manager training and awareness (both as handlers of data, guardians of department data and champions of best practice) with Information Governance (CR/VH) and HR (Caroline Newman).**

f. **Review threat landscape (new agenda item)**

The Committee did not have any current concerns regarding risk of widespread use of storage mediums (including personal Dropbox).

4. **Any other business**

PG highlighted the regular Campus IT meetings as a useful way for IT providers to pool ideas and learn from each other.

5. **Date of next meeting**

RB noted that this Committee reports into the School IT Committee which meets on a termly basis in November/December, March/April and June/July. He recommend that this Committee should therefore meet for the next time in mid to late September followed by mid to late February. The meeting in February would enable them to support the NHSPT for all safe havens. The Committee agreed to this proposal.