Information Security Oversight Committee
Friday, 26th May 2017

Present: Richard Bartlett (RB), Kieran Lovell (KB), Stephen Jones (SJ), Rich Hutchinson (RH), Guy Williams (GW), Carolyn Read (CR), Lydia Drumright (LD), and Stefan Graf (SG).

1. Apologies
   a. Peter Gibbin (PG)

2. Minutes and actions from last meeting
   a. Toolkit access via purchase orders done
   b. LD action unknown, but CR said LD is pushing for a policy at University level
   c. Ref policies, KL raised RIP bill, and we may be in scope, KL to raise with Martin Bellamy that UCISA/JISC/Legal Services needs to be involved in this decision.
   d. KL done action to create policy page, RB pickup in School site
   e. KL talked to mobile device management, CL against control
   f. CR induction package, CR check, RB check as well, SG says Haem is really good, that's the bar, need to check whether everything
   g. KL raised external lookup opt in, seems to be everyone opted in by default
   h. RB not done, KL going on course, KL/RB come up with something in default
   i. RB action on breach, not done, still unclear, KL talk to James Knapton, RB address concerns about reporting

3. Objectives
   a) Setting Policy
      i. UIS Organisational Framework
      ii. UIS Information Loss Reporting Framework
         i. When does James get informed? Make sure he's happy with the policy
      iii. Policy Development Process
         i. Pointed out how this will work for web hosting policy
      iv. CSCP incident, NetNames and Web Hosting Policy
         i. Covered above
   b) Reviewing Implementation
      i. Not a lot of resource to do this by end of February, KL suggested Cyber Essentials Plus, <£1k
      ii. RB will raise the fact that we don't have enough money to do this
c) Review of Safe Havens
   i. End of March is the deadline, may be able to do it by then
   ii. We've changed the way some of the toolkit implementations works, more work to be done
   iii. User consultation in researchers key to designing and developing these systems
       i. GP's bad at protocol, CCG's had to be informed when PID went nhs.net > cam.ac.uk (which is a brief)

d) Maintaining Information Governance Toolkit
   i. Quite a lot of policy change to allow for new use cases, will make the implementation review difficult

e) Review Breaches
   i. How do we find out if there's a breach? SG said he has collaborators who use data on the HPC, they sign a document that says they won't copy data out, SG talked to Stuart Rankin, who said this is really hard to do. Too many egress points in the HPC.

f) Review threat landscape
   i. Ransomware
   ii. Sophos/UIS

4. Any other business
   a. Potential solutions
   b. Training and awareness
      i. RH OK, Field staff
      ii. GW depends on the user, some more aware, Radiographers
      iii. SG technical users only, signed agreement, a lot is read only, restricted groups have access. Everything with co-ordinators etc. involved, using OwnCloud etc. that's where the risk is. Stuart Meacham does awareness raising every 2-3 weeks. Biologists more at risk.

   c. Consultation methods
      i. Research Nurses need to be happy that it works
      ii. 5. Revocation of accounts isn't warning, if we still warn then they'll be happy with that.

5. Date of next meeting
   TBC