|  |  |
| --- | --- |
| **Agenda item:** | **4** |
| **Attachment:** | **B** |

**HRA BOARD COVER SHEET**

|  |  |
| --- | --- |
| **Date of Meeting:** | 19 July 2017 |

|  |  |
| --- | --- |
| **Title of Paper:** | Matters arising - Board Briefing on Cyber Security Risks |
| **Purpose of Paper:** | To note the report and ask any questions |
| **Reason for Submission:** | In response to specific Board request:  *The Board noted the recent cyber-attack on some NHS organisations and confirmed the HRA had not been affected. The Board noted the cyber related risk was not currently on the corporate risk register however was assured the risk was captured and mitigated at the directorate level risk register and was therefore below the threshold for escalation to the Board. The Board noted the Audit and Risk Committee had discussed cyber risk at a recent meeting and there had been a Health Group Internal Audit on cyber risk last year, with relatively robust arrangements in place. The Board however noted the risk was constant and dynamic and invited management to check the risk was at the correct level following the recent event. The Board discussed the training provided in relation to information governance and queried if there was any specific training in relation to phishing emails.*  ***Action: Update on cyber-risk and related training to be brought as matter arising to next meeting*** |
| **Details:** | **HRA INFORMATION ASSETS**  There are 17 HRA information assets recorded ranging from REC Paper records to IRAS and HARP.  The key business critical systems are the Integrated Research Applications System (IRAS), the HRA Assessment Review Portal (HARP), the ATOS systems (a managed service environment providing controlled access to email (NHS Mail via Outlook), internet, intranet, shared drives and other bespoke / dedicated software), and the Finance and HR systems.  The HRA has sole responsibility for IRAS and HARP and is the data controller. BGO are contracted by the HRA to manage the systems, with Rackspace (soon to be Crown Hosting) providing the supporting hardware infrastructure.  The ATOS managed service is contracted by the Department of Health with the HRA, along with other ALBs, being an active member of the contract management group.  The Finance and HR systems are managed by NHS Shared Business Services (SBS) and NHS Business Services Authority (BSA) under National Contract that individual NHS entities buy into. Again the HRA is an active member of the contract management group.  **RISKS**  The vulnerabilities exposed by the recent attacks on NHS systems were primarily due to outdated, unsupported operating systems without the latest and relevant security updates (if supported at all), combined with phishing attacks.  The only business critical system the HRA has that is potentially affected by these vulnerabilities is the ATOS managed service as email is a core product. To review and address these vulnerabilities, the HRA IT support department have been working closely with ATOS and other ALBs within the Contract Management Group to ensure the systems are kept secure. These include:   * a check that the Microsoft Windows operating system (Windows 7) is not susceptible to the same or similar vulnerabilities; * a check that all partner manufacturers and suppliers have updated their systems; * ensuring that all relevant system security patches and updates are implemented with all going through a robust RFC and CAB process; * that network availability and security has been checked and updated; * a check that all laptops have updated anti-virus software; and * communications with staff to ensure their laptops are kept updated.   ATOS and its partner organisations have been very responsive and have worked hard to review the systems security since the attacks.  All HRA laptops are updated automatically as soon as they connect to a network. In the unlikely event that a laptop has not been connected, the laptop will be quarantined.  It is our view that these activities have mitigated the risks of a successful cyber-attack on these systems to an acceptable level.  Gross risk assessed as Likelihood 4 Impact 4 = 16  Net risk assessed as Likelihood 2 Impact 4 = 8  We can confirm that the Mandatory Training provided to staff through the Civil Service Learning packages includes specific and comprehensive training in relation to phishing emails. In addition mandatory training, regular communications to staff and supporting guidance information on the Intranet helps maintain a good level of awareness of the risks amongst staff.  With regard to the other business critical systems, The Information Governance Steering Group (IGSG) recently reviewed and approved the “HRA IT Security Plan” which governs the integrity, and security of the HRA’s information stored in the databases linked to the systems HARP, IRAS, GFI and TOPS. As such it conforms to the HMG Security Policy Framework. The document details the governance arrangements, roles and responsibilities, training and policies and procedures and processes; which include access control, hardening of servers, penetration and ethical hacking testing, anti-virus testing, back-up and restore, and disaster recovery to name but a few. Recent work includes increasing the patching of the Window server software to twice a month to ensure the software is up to date and also enhancing the software to mitigate vulnerabilities recommended by the penetration testing  The IGSG was therefore assured that the control environment under which HRA systems are managed is robust and fit for purpose and the mitigations reduce the risks of a successful cyber-attack to an acceptable level.  Gross risk assessed as Likelihood 3 Impact 4 = 12  Net risk assessed as Likelihood 1 Impact 4 = 4  Finally, for the Finance and HR systems, substantial assurance is provided through the regular performance monitoring meetings between the HRA and these bodies and the national framework contract which includes stipulations for system security and safety under which the systems operate within BSA and SBS. Again, the assessed level of the risk of a successful attack against these systems is low from the HRA perspective.  Gross risk assessed as Likelihood 4 Impact 4 = 16  Net risk assessed as Likelihood 2 Impact 4 = 8  In summary, as Senior Information Risk Owner (SIRO), I can report to the Board that I, supported by the Information Governance Steering Group, have assessed the overall risks to the HRA’s critical business IT systems and concluded that the mitigations in place to manage the associated cyber risks are robust and fit for purpose and the risks have been reduced to levels that are acceptable and do not need to be addressed within the Corporate Risk register. This does not mean that a cyber-attack will not happen nor that it will be unsuccessful, but the Board can be assured that the HRA is working hard to help reduce the risk of it happening and to mitigate the impact on the HRA and the research community if the risk were to materialise. |
| **Time required for item:** | **15** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Recommendation / Proposed Actions:** | **To Approve** | |  |
| **To Note** | | **x** |
| **For Discussion** | |  |
| **Comments** |  | |

|  |  |
| --- | --- |
| **Name:** | Stephen Robinson |
| **Job Title:** | Corporate Secretary and Senior Information Risk Owner (SIRO) |
| **Date:** | 10/07/2017 |