**Ref: GJF/2018/03/08**

# GJF Logo

# Board Meeting: 27 March 2018

**Subject:** Cyber Resilience – Public Sector Action   
Plan

**Recommendation:** Board Members are asked to note the recommendations as highlighted in the paper and support the implementation of the action plan

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**1 Background**

Following the global cyber attack in May 2017 (Wannacry) and the significant impact on NHS Services in Scotland, the Scottish Government and the National Cyber Resilience Leaders’ Board have developed a Public Sector Action Plan for Cyber Resilience. It sets out the key actions that the Scottish Government, public bodies and key partners will take, up to the end of 2018, to further enhance cyber resilience in Scotland’s Public Sector.

A letter was issued from Deputy First Minister, on 8 November 2017, to NHS Boards Chief Executives, with a copy of the action plan, requesting that appropriate steps are taken to implement within the timescales set out in the plan.

In addition, it was requested that a senior member of our board or executive team take overall responsibility for delivery of the action plan. We have confirmed that the Director of Finance, in her role as Senior Information Risk Owner (SIRO), will lead this implementation programme.

**2 Assessment**

A copy of the action plan has been attached as Appendix 1.

The action plan has been reviewed and assessment of current status and actions required to support implementation by the required timescales has been made and RAG status assigned.

One of the key actions is to have, in place, appropriate independent assurance of critical cyber security controls (Cyber Essentials) by the end of October 2018. To support this action, an independent pre-assessment of our critical cyber security controls will take place by the end of March 2018.

In addition, there are a small number of recommendations which would support the implementation of the action plan.

**2.1 Cyber Security Training**

To date, 10 courses have been delivered in partnership with Counter Fraud Service. Attendance at each session has been around 15, totalling 158 which is lower than we have liked. In order to encourage wider attendance, the Senior Management Team (SMT) has approved the proposal that this training should be made mandatory for, at least, all corporate staff, in the first instance, who have regular access to email and are therefore at risk of activating emails/links which contain malware. In addition, all Executive and Non Executive members of the Board will be invited to attend training.

**2.2 Process for dealing with ‘frequent’ offenders**

Through review of recent potential threats to IT security via emails, it has been highlighted that a small group of staff repeatedly click on attachments despite communications around the need to be vigilant.

SMT has approved the development and implementation of a process, similar to that which is in place with FairWarning. This process will identify staff who repeatedly activate phishing emails/links, will support the provision of additional training to groups or individuals, will enable feedback to managers and if repeated would potentially lead to a disciplinary process. This process will be developed in conjunction with HR and Partnership Forum.

**2.3 Policy for the management of infected devices**

Where cyber attack has been detected, it is critical that infected devices are quarantined and remedial action taken. The overhead for the eHealth team to action is significant, for example, the recent malware attack through email took in total 150 hours (20 days) to remediate.

SMT has approved the development and implementation of a policy for the management of infected devices by the eHealth department, This policy will highlight the steps to be taken where devices are infected and the recovery timescales.

**2.4 Cyber Essentials plus accreditation**

SMT are supportive of the proposal that the Board should obtain Cyber Essentials plus accreditation. This certification scheme offers a mechanism for organisations to demonstrate that they have taken essential precautions against cyber threat and is strongly preferred by Scottish Government and the National Cyber Resilience Leaders’ Board.

The cost of accreditation is £5000.00, which will be met from eHealth strategic fund, and should be obtained by October 2018.

**2.5 Purchase of automated patching system**

Currently, the implementation of security patches is undertaken manually, usually every Thursday evening. This requires eHealth staff to work outwith core hours to apply these patches to business critical systems. The cost per annum of this approach is approximately £12,000.00

SMT has approved the purchase of an automated patch management system which will allow patches to be applied automatically, on a regular basis. In addition, the system provides real time reporting on IT assets such as, the number of devices successfully patched and those which may pose a risk to the organisation.

Automated patch management is recommended as one of the cyber security control measures and has been implemented in a number of NHS Boards.

Total cost of this system is approximately £25,000 for a three- year licence.

**3 Recommendations**

Members are asked to note the recommendations and the implementation of the action plan.

**Julie Carter**

**Director of Finance**

**2 March 2018**

**(Sally Smith, Head of eHealth)**

**Appendix A – Public Sector Action Plan for Cyber Resilience**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Key Action** | **Responsible Body** | **Requirements** | **Deadline** | **RAG**  **Status** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Preparatory** | * ALL | All bodies to provide contact details of 1) Board/Senior Management, 2) working level, and 3) incident response to the SG Cyber Resilience Unit | November 2017 | **complete** |
| Key Action 1 | * SG * NCRLB * NCSC * SPSCC | To finalise Scottish Public Sector Cyber Resilience Framework.  This will:   * Provide a common approach * Align with new NIS guidance * Take account of foreseeable technological developments * Minimise additional burdens * Provide clarity and assurance   It will cover 4 key domains of cyber resilience:   * Identify * Protect * Detect * Respond & Recover | June 2018 | **on track to complete by deadline**  Review of the high level concept framework completed. |
| Key Action 2 | * GJF | All bodies must have in place Board/Senior Management commitment to manage risks from cyber threat.  Minimum appropriate governance arrangements in place:   * A named Board/Senior responsible manager * Regular Board/Senior Management level consideration with appropriate policies and processes | June 2018 | **on track to complete by deadline**  Director of Finance confirmed as SIRO  Head of eHealth confirmed as point of contact for incidents  Review of all current policies and procedures underway |
| Key Action 3 | * GJF | For all Boards to join Cyber security Information /sharing Partnership CiSP  For all Scottish Boards to then join the Community Group within CiSP Scottish Cyber Information Network SCiNET | June 2018 | **complete**  Registered with CiSP.  Registered with SciNET |
| Key Action 4 | * GJF | To ensure you have appropriate independent assurance that critical technical controls are in place.  Adoption of, as a minimum, five critical network controls; **Boundary firewalls and internet gateways, Secure configuration, Access control, Malware protection, Patch management.**   * Undergo **Cyber Essentials “pre-assessment”** funded (to defined limits) by Scottish Government * Decide whether to pursue Cyber Essentials or Cyber Essentials Plus Certification * Achieve the agreed certification | March 2018  April 2018  October 2018 | **on track to complete by deadline**  Pre-assessment by independent reviewer arranged for w/b 19th March  Recommend Cyber Essential plus certification to SMT |
| Key Action 5 | * GJF | Ensure appropriate implementation of Active Cyber Defence measures.  Free to use measures under the Active Cyber Defence programme:   * Protected DNS * DMARC anti-spoofing * Webcheck * Phishing and malware mitigation   SG will work with Board’s to raise awareness of these services.  Alternative solutions can also be used. | June 2018 | **on track to complete by deadline**  **Protected DNS**  Currently being progressed by Scotland Wide Area Network Provider (SWAN)  **SPF (DMARC, DKIM, TLS)**  Currently in progress. Current email system under review to ensure compliance.  **Webcheck**  Websites owned by GJF currently being checked    **Phishing and malware mitigation**  Products deployed.  Ongoing training delivered to raise staff awareness. |
| Key Action 6 | * SG * GJF | SG to provide awareness and training and materials for use by public bodies.   * Arrangements in place for appropriate training * Implement core training to all staff * Ensure appropriate disciplinary procedures are in place | March 2018 – 2020  March 2018  June 2018  June 2018 | **on track to complete by deadline**  10 workshops held in conjunction with CFS  Further schedule planned – twice monthly sessions |
| Key Action 7 | * SG * GJF | SG, working with NCSC and Police Scotland to support public bodies with implementing Cyber Incident Response Policies and Plans.  SG will put in place specialist training to support the development of skills in respect of cyber security incident response  GJF must have in place a Cyber Incident Response Policy and Plan in place and these must support the incident notification and coordination protocols | June 2018 | **complete**  Policy and Plan in place to ensure capture of notification protocols. |
| Key Action 8 | * SG * GJF | SG will develop a policy in respect of supply chain cyber security which should then be applied by public bodies.  Guidance will also be developed on the need for recipients of public grant funding to have in place proportionate and risk based cyber security arrangements  GJF to implement Procurement Policy Note and Grant funding guidance.  Guidance on existing contracts conformity will be provided by SG | May 2018  June 2018  June 2018 | **on track to complete by deadline**  SG to provide policy and guidance to all public authorities on compliance for external contractors / suppliers  Currently reviewing register of existing suppliers.  Standard clauses for contracts are being amended with support from CLO and will be forwarded to all Boards |
| Key Action 9 | * SG | SG to put in place Dynamic Purchasing System for digital services for public bodies to use. | October 2017 | **Complete**  System now displayed on SG website. |
| Key Action 10 | * PSCC * GJF | Finalise the Public Sector Cyber Resilience Framework identifying key challenges  Key public bodies identified as Public Sector Cyber Catalysts  GJF to implement and report against Framework | June 2018  2017  June 2018 | **on track to complete by deadline**  Feedback from Cyber Catalyst organisations is being collated by national Information Security Forum and will be shared with all Boards |
| Key Action 11 | * SG * GJF | SG will put in place effective monitoring and evaluation to help assess progress against this action plan and also the Framework, once developed.  GJF required to:   * Provide informal, working level responses to SG enquiries * Provide one off written assurance at SMT/Board level on the following: * Confirmation of (i) having undergone a Cyber Essentials pre-assessment, (ii) having taken a decision on whether to seek Cyber Essentials or Cyber Essentials Plus, and (iii) the expected timelines for achieving this. * Board/Senior Management level commitment and basic governance arrangements. * CiSP membership. * Appropriate use of Active Cyber Defence measures. * Appropriate training and awareness raising processes. * Cyber incident response protocols, aligned with central mechanisms. * Provide **one-off written confirmation** that Cyber Essentials or Cyber Essentials **Plus** certification (or, exceptionally, alternative independent assurance) has been achieved. | June 2018  October 2018 | **on track to complete by deadline**  SG will put in place effective monitoring and evaluation to help assess progress against this action plan and also the Framework.  GJF will provide informal, working level responses to SG enquiries and will also provide one off written assurance at SMT/Board level on compliance.  The status on the following areas are:  **Cyber Essentials**  Independent provider commissioned to carry out pre-assessment and Essentials Plus accreditation.  **Board Commitment**  SIRO confirmed with regular updates to Information Governance Group & SMT  **CiSP**  Completed  **Active Cyber Defence measures**  Currently utilising Sophos suite of products and tools provided by the NCSC.  **Training**  Ongoing training to be delivered to raise staff awareness.  **Cyber incident response**  GJF Cyber Incident Response Policy and Plan updated to reflect change to reporting, to include NCSC. |