31st May 2017

Neil Findlay MSP
Convener
Health and Sport Committee
T3.60
The Scottish Parliament
Edinburgh
EH99 1SP

Letter sent by e-mail to: healthandsport@scottish.parliament.uk

Dear Mr Neil Findlay,

RE: IT Cyber attacks

1. What impact did the recent cyber-attack have on your organisation and the public?

As a result of the global cyber-attack which was first identified on the afternoon of Friday 12 May, Healthcare Improvement Scotland’s initial focus was on trying to block the attack. As a precautionary measure our servers were shut down on Friday afternoon and over the weekend to protect our infrastructure, hardware, local and national systems. During this time the systems were fully checked and found to be virus free. On Sunday 14 May the focus moved to planning for start of business on Monday 15 May. The objective was to prevent any virus being introduced to the systems and we instigated a process of checking all (473) devices and applying patches (which are released when it is discovered that there is a threat to the system) prior to them being allowed access to our networks.

Our Business Continuity fixed site incident plans were used for communicating with staff and developing a robust patching process across our two main sites. The patching process was operational in both sites first thing on Monday with each device taking roughly 20 minutes. The available resource restricted this process to patching no more than 30 devices per hour across both sites and the procedure was in place for a few days to accommodate staff who were not able to visit an office immediately. On Monday 16 May there was also a 5 hour delay to gaining access to our drives on the servers due to a subsequent hardware failure at the NSS datacentre.

With regard to Healthcare Improvement Scotland there was no direct impact on the public as a result of the global cyber-attack. This includes the regional offices within the Scottish Health Council. To remove the burden on NHS boards, an inspection due to take place week beginning the 15 May was cancelled and rescheduled. Healthcare Improvement Scotland also has staff working on Death Certification based within NHS24 premises at Cardonald in Glasgow. The Death Certification team did experience problems between the NHS24 systems and those of the Registrar of Scotland. A manual contingency plan which had previously been tested was in place for 5 working days. The manual contingency did not result in the delay of any funerals and there is no evidence that suggests there was any impact on the public.

NOTE: ransomware was not detected on any of the Healthcare Improvement Scotland devices that were scanned and patched.

2. Following the cyber-attack how has your approach to prevention of such attacks been revised?

Healthcare Improvement Scotland will continue to assess its operations and identify ways in which it could minimise or prevent any future attack. In particular, regular reminders will be issued to staff regarding the process to be taken if suspicious emails are received. The organisation had recently reviewed its patching strategy to be prepared for such an attack and in a pre-planned action we had purchased updated versions of SCCM (System Centre Configuration Manager) and WSUS (Windows Server Update Service) patching software tools.
Our IT staff will now receive more frequent updates from our national ehealth leads on any cyber security concerns and IT will regularly monitor all recommended Microsoft updates. IT will also look to increase collaborative working on patching management across other NHS Boards. We will continue to supply information through Freedom of Information (FoI) requests but will remain vigilant when providing technical information which could pose a risk to our cyber security.

3. **What additional support would assist in preventing such attacks?**

We have identified several areas where we believe improvements could be made to help prevent such attacks.

- more frequent updates and national alerts to public services from the national cyber-crime unit
- the development of an improved national vulnerability scanning tool
- the creation of a centre of excellence with key skilled personnel to provide support or advice within the public sector
- the centre of excellence could include a national download or update centre
- there is further scope for greater collaboration with NHS boards
- additional resource or working differently may be required for patch management and increasing cyber security activity

4. **To what extent do you collaborate with other Boards on IT security issues?**

Healthcare Improvement Scotland is a member of the four major national NHS IT groups that discuss security issues: the Scottish Telecommunications Advisory Group (STAG) national networks group, ehealth leads group, Information Governance and the National Infrastructures Leads group. Our IT service is managed by the Scottish Ambulance Service (SAS). The service level agreement with the SAS encourages the sharing of skills, knowledge and information relating to all aspects of IT development which includes cyber security. HIS also share networks with NHS National Services Scotland (NSS) which requires collaborative working and cross organisational cyber security cooperation.

Yours sincerely,

Robbie Pearson
Chief Executive