Scottish Ambulance Service
Taking Care to the Patient

NHS SCOTLAND

Chair David Garbutt QPM
Chief Executive Pauline Howie OBE

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

26 May 2017

Dear Mr Findlay

IT CYBER ATTACKS

I refer to your letter of 19 May in relation to the recent cyber-attack and the impact on the Scottish Ambulance Service.

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

The cyber-attack on 12 May 2017 exploited a vulnerability in a number of versions of the Microsoft Windows operating system e.g. Windows XP, Windows 7 and Windows 8.

On hearing of the cyber-attack in other parts of the NHS, the Service's *Information Security Incident Response Team (ISIRT)* was immediately stood up and it was quickly established that out of over 3,350 Windows devices within the Service estate, 14 desktop PCs and 1 laptop were infected. These were removed from the network on 12 May and replaced by 15 May. No patient services were impacted as it was station / admin PCs that were infected. Precautions around access to email and telemetry were introduced, and normal working resumed over the weekend and fully by 16 May.

On 15 May, our General Manager ICT provided a statement to Police Scotland in relation to the cyber-attack.

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

Our overall approach to the prevention of a cyber-attack remains unchanged at the date of this letter. We have, however, checked the patching status of our complete ICT estate since the attack and revised systems and protocols will be introduced to ensure that all systems and hardware devices are operating on the most recent patch release. Utilising the services of our National Risk and Resilience team we plan to conduct a full structured debrief following the attack.

3./

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

Cyber attacks are now a part of modern life with attacks of one form or another occurring every day. Many of these attacks exploit vulnerabilities in Microsoft Windows operating systems. Cyber attacks of the scale seen on 12 May 2017 are much less common. The National Cyber Security Centre (NCSC) has recommended that all organisations take some immediate actions to counter the current threat. Their recommendations can be summarised as:

- Keep security software patches up to date;
- Use proper antivirus software services; and
- Maintain back-ups of critical data.

Our ICT Team currently has a patching regime in place although we are seeking to improve our overall control environment by ensuring that all appropriate patching has been undertaken. We utilise a range of sophisticated antivirus software packages and the ICT team currently has a robust data back-up regime in place.

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

We have representatives that regularly attend the eHealth IT Security group, eHealth National Infrastructure group and the eHealth Leads group. Discussion at these groups regularly cover IT security issues and allows the sharing of knowledge and experience between attending boards relating to all IT issues and not just security.

There has recently been discussion at eHealth Leads meetings regarding setting up an ICT Security 'Centre of Expertise' within NHSS, with the aim being to use the shared services approach to providing NHSS Boards access to specialist advice and services. The Scottish Ambulance Service fully supports this approach.

I trust that this information helps the Committee in its future deliberations and we will of course provide any further information that you may require.

Yours sincerely

Pauline Howie, OBE
Chief Executive