Borders NHS Board

CYBER-ATTACK MAY 2017

Aim

The aim of this paper is to brief the Board on the early findings and impact of the Cyber-attack of 12th May 2017. A fuller post incident review is planned over coming weeks.

Background

On Friday 12th May, NHS Borders, along with much of NHS Scotland and organisations across the globe, were the subject of a ransomware attack. Forty seven PCs and one fileserver across three Community locations were affected and the main file store had a small number of files encrypted.

IT teams responded quickly to isolate and contain the spread of the threat and an incident team was convened to manage the incident and its impact on services. The locations were, Hawick Health Centre, Hawick Hospital and the Learning Disability Service at Earlston.

The ransomware was unprecedented in its scale of impact as it took advantage of Microsoft security vulnerability and was able to spread from computer to computer rather than the more usual means of infecting individual PCs via a user activating a web link within an email.

Teviot Medical Practice was unable to see patients from around 2:30pm on Friday 12th May as their main computers had been shut down to prevent further spread of the malware.

Intensive work took place over the first weekend to recover the affected locations to a point where staff could provide a near normal service from Monday 15th May.

At the same time work commenced to secure NHS Borders equipment from spread and further attack by this malware. Full recovery of all locations took place over the period concluding on Friday 26th May when all infected equipment had been replaced.

Scottish Borders Council, NHS Fife and NHS Lothian provided assistance and staff to help the local IT team with the volume of work during the first few days of the incident.

A small number of patients across services at affected locations had appointments rescheduled to alternative dates.

As the main fileserver was isolated while it was checked for malware, many services were affected by a lack of access to files stored there. This had an impact on the wider organisation. For some this was immediate or soon after the event and became more

critical with time, for others the impact is less obvious causing delays and work backlogs. It may take some time before the full impact is known and felt by the organisation.

Clearly there was also an impact on the IM&T team who worked tirelessly to restore normal operations to the organisation, leaving routine and project work to focus on the incident. The team will continue to be impacted by a backlog of routine calls made to the service desk both during the incident and in subsequent weeks.

While the situation was extremely challenging for both affected services and IT teams, staff coped well in difficult circumstances offering as much as was possible using contingency plans.

Summary

This was an incident which had the potential to have a much larger impact on patient care than it did. NHS Borders staff were quick to recognise the threat, take steps to contain it and mobilise a team to manage the incident and its impact.

Our partners in the NHS and the local authority responded quickly to our request for assistance.

Both affected services and the wider staff group responded well & positively during the incident to ensure that the organisation functioned as normally as possible.

NHS Borders is protected from this malware and work continues to review our security to ensure we are protected from further threats.

The Board will recall that further improving security & resilience are key drivers within the IM&T Roadmaps and Investment Plan and they approved at their Strategy & Performance Committee meeting on 4th May and work is underway to start to deliver this.

A full post incident review will take place in the next few weeks and recommendations will be taken forward, technically and organisationally as appropriate.

Recommendation

The Board is asked to **note** the content of this paper.

Policy/Strategy Implications	N/A
Consultation	
Consultation with Professional Committees	N/A
Risk Assessment	Further risk assessment will be completed as part of the post incident review.
Compliance with Board Policy requirements on Equality and Diversity	An impact assessment has not been carried out as this was an unforeseen event.
Resource/Staffing Implications	To be determined as part of the post incident review once full impact is known.

Approved by

Name	Designation	Name	Designation
June Smyth	Director of Planning & Performance		

Author(s)

Name	Designation	Name	Designation
Jackie Stephen	Head of IM&T		