POLICE & CRIME COMMISSIONER FOR LEICESTERSHIRE JOINT AUDIT, RISK & ASSURANCE PANEL

Paper Marked

A

Report of	**OFFICE OF CHIEF CONSTABLE**
Subject	**PATCHING UPDATE**
Date	**THURSDAY 14th SEPTEMBER 2017 – 2.00 P.M.**
Author	**DCC BANNISTER**

Purpose of report

1. This report provides JARAP with information about the Leicestershire Police response to the recent NHS cyber-attack.

Recommendation

2. The panel is asked to note the contents of this.

Overview

3. On 13th May 2017 the NHS were subjected to a ransomware cyber-attack, which took advantage of known software vulnerabilities.

4. A number of key safeguards are already in place in order to try and prevent and if successful minimise the impact of a cyber-attack upon Leicestershire Police:-

- Anti-virus scanning with up to date signatures on external e-mail, web browsing traffic, desktops, servers and laptops.
- Network has two controls in place to prevent bypassing web and e-mail controls.
- The spam control is implemented.
- Mail and web controls prevent users receiving or downloading mobile code.
- The patches for MS17-010 have been deployed (this was the vulnerability to the NHS as the patch had not been completed).
- We have resourced on-call in the event of an incident that can mobilise additional resources to deal.
- We have disaster recovery and business continuity plans tested and in place.
- Regular intranet messages reminding users of their responsibility to scrutinise messages and not click on links or attachments in suspicious e-mails.

5. Leicestershire Police was not affected – the Head of IT clarified that we would have known if an attempt had been made.

Leicestershire Police response

6. The IT department took swift action and responded outside of office hours to safeguard the force, with updates coordinated with the business, the Chief Officer Team and NPoCC via the designated silver commander. The activities were undertaken as follows:-

- Patches for MS17-010 and MS17-008 confirmed as deployed for all workstations.
- Additional blocks put in place on mail marshal and web marshal to block the specifics of the malware.
- Mail and web marshal AV updating confirmed.
- The kill domain available to force machines via web marshal.
- Two intranet messages published with advice to users.
- Increased opening hours for IT helpdesk to deal with increase in queries and concerns from staff.
- Personal email to all staff from DCC Bannister reiterating comms messages.
- Desktop and server AV deployment confirmed up to date and detecting.
- CMD asked to be vigilant and suspicious of any mail with attachments as the main portal into the organisation over the weekend.

Learning through debrief

7. A crisis management team meeting was held, to debrief all relevant stakeholders and identify any additional actions required.

8. A strategic risk has now been added to the risk register outlining the risk of cyber-attack to Leicestershire Police. It has been assessed as impact high and likelihood medium, providing an overall score of medium (6). Mitigation controls are in place and the risk remains under routine review by the Head of IT.

9. A regional IT cyber-attack table top exercise is being planned by the force Business Continuity Advisors to explore the impact upon shared services and the response by the various stakeholders within each force. The outcome of this exercise and learning will be shared with the Deputy Chief Constables Board and internally with the Strategic Organisational Risk Board (SORB).

Implications

Financial - Nil

Equality impact assessment
- Nil

Risks and impact - STR1991 Threat of cyber-attack

Link to Police and Crime Plan - Nil

Appendices

Nil

Persons to contact

Roger Bannister – Deputy Chief Constable – (0116) 248 2005
Email: Roger.Bannister@leicestershire.pnn.police.uk