INFORMATION

RIBBLE VALLEY BOROUGH COUNCIL
REPORT TO ACCOUNTS AND AUDIT COMMITTEE

Agenda Item No

meeting date: 26 JULY 2017
title: RESPONSE TO GLOBAL CYBER ATTACK MAY 2017 (WANNACRY)
submitted by: DIRECTOR OF RESOURCES
principal author: STUART HAWORTH

1 PURPOSE

1.1 To inform members of the Council's response to the global cyberattack that occurred during May 2017.

2 BACKGROUND

2.1 The attack began on Friday, 12 May 2017, and within a day was reported to have infected more than 230,000 computers in over 150 countries. Parts of the United Kingdom's National Health Service (NHS), Spain's Telefónica, FedEx and Deutsche Bahn were hit, along with many other countries and companies worldwide.

2.2 WannaCry made use of a vulnerability (Eternal Blue) within Microsoft's operating systems. Eternal Blue was discovered by the U.S National Security Agency (NSA). Rather than reporting the vulnerability to Microsoft, the NSA used it in their cyber offensive work. Microsoft eventually discovered the vulnerability and released a security patch in March 2017 for all supported version of the Windows operating system.

2.3 Organisations affected by WannaCry were either using outdated Microsoft operating systems or hadn't applied the patch released by Microsoft.

2.4 The WannaCry ransomware attack was a worldwide cyberattack, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments.

3 HOW RIBBLE VALLEY'S ICT INFRASTRUCTURE IS PROTECTED

3.1 As a matter of course the Council has a number of procedures and technologies in place to protect the Council's ICT infrastructure.

- The Council ensures that all computer systems that connect to the authority's infrastructure, regardless of operating system, are protected from malicious code and/or hacking attacks through the deployment and installation of operating system patches.
- Firewalls are installed on all connections to third party networks.
- Firewalls are configured with the minimum number of services to allow for the Council's business to function.
- The Council ensures that all computer systems have a current and up to date antivirus product installed and that a full virus scan of equipment is performed on a regular basis.
- Emails that traverse the Council's ICT infrastructure have their content inspected.
- Any public facing services (web servers) are placed in a network that is separate to the corporate network.
- Regular system backups are taken and copies stored off-site.

- All users who use the Council's ICT infrastructure sign the Council's ICT usage policies.
- Annually a penetration test and ICT health check are performed by an external organisation to test the security of the Council's infrastructure.

4 HOW RIBBLE VALLEY WAS PROTECTED FROM WANNACRY

4.1 As the WannaCry cyberattack developed over Friday 12 May and Saturday 13 May it was felt by the ICT Manager that it would be prudent for extra checks to be taken to ensure that the Council's infrastructure would not be affected by the outbreak.

- A patch audit was conducted to ensure that the necessary Microsoft patch had been applied.
- A teleconference between the ICT Manager and the ICT Infrastructure Officer took place to devise an appropriate response to the cyberattack. From that conversation the following actions were agreed:
  - That over the weekend all servers would be fully patched regardless of whether the patch specific to the ransomware attack had been applied.
  - That all users of the Council's network infrastructure be locked out until all desktops/laptops had been fully patch audited and any outstanding operating system patches applied.
  - That the level of automated protection on the corporate firewalls be increased.
  - That all incoming email be quarantined to allow ICT staff the opportunity to check that they were free from infection.
- During the course of Monday 15 May, ICT staff visited every desktop/laptop computer to check that any outstanding patches were applied.
- Public facing services were the first to be checked to minimise disruption.
- In total 181 desktops/laptops were checked by ICT staff.

4.2 By 19:30 on Monday 15 May normal service was resumed throughout the council.

5 CONCLUSION

5.1 The council was not directly affected by the WannaCry cyberattack, but was impacted only by the timely precautionary measures taken by the ICT team.

5.2 It is inevitable that there will be future cyberattacks, which will become more sophisticated and harder to deal with. Good practice, user training and the introduction of new technologies will help to ensure that systems are kept secure in the future.

ICT MANAGER DIRECTOR OF RESOURCES

AA15-17/SH/AC
11 July 2017