REPORT TO: **JOINT AUDIT AND ETHICS COMMITTEE**

DATE: **11 December 2017**

REPORT AUTHOR: **Mr Adrian Emberton, Supt. E Newton**

SUBJECT: Network & Cyber security within Lancashire Constabulary

1 Issue for Consideration

1.1 Members of the committee requested information in relation to the security and technical controls in place following the NHS cyber-attack earlier this year

2 Recommendation

2.1 That committee notes the report

3 Background

3.1 How secure is Lancashire Constabulary? There is no simple answer to this, and it is difficult to quantify, due to the ever-changing nature of cyber threats, an ever-increasing use of digital information, and constantly evolving technology. Information Security is concerned with three core pillars – the Confidentiality, Integrity, and Availability, of information.

3.2 When implementing systems and assessing risk, all three elements are addressed, although it is broadly acknowledged that the pillars are often discordant with one another - for example – by making information more *available* this may increase the risk of breaching its' *confidentiality*. It follows that in order to operate effectively as an organisation - which is heavily reliant upon accessing and processing digital information - it is not possible to eliminate *all* information security risks.

3.3 In terms of technical infrastructure, Lancashire Constabulary is categorised as an enterprise[1] environment with over 10000 end-points[2] and over 250 applications. This in

[1] An enterprise network is a large computer network built to share IT resources and information across the entire organisation
[2] An end-point is any device that can connect to the Lancashire Constabulary network

turn connects to the much larger police community across national networks, to exchange information with other organisations and consume services, e.g. PNC, and ANPR. Hence, the environment is complex, and often difficult to protect and manage.

3.4 Traditional security models considered a 'clam shell' approach, whereby the outer network perimeter is heavily guarded, but minimal security was implemented once inside the network (hence the clam shell - hard on the outside, soft in the middle.) However, it is now considered that with the proliferation of Internet, Email, and Cloud-based services, the network boundary has significantly blurred. As such, Lancashire Constabulary have adopted a 'Defence in Depth' approach to its security; implementing several layers of security controls, rather than a single line of defense. This mitigates the concept that a simple breach of the perimeter could compromise the entire network; rather, an attacker would have to penetrate several different defense mechanisms, requiring more time, resources, and skill

3.5 The consequences of a large-scale cyber-attack cannot be underestimated and proposals to increase our resilience has been accepted by the Chief Officer Group and Senior Managers. A plan of works is currently underway that will span the next 12-months; overseen by the Senior Information Risk Owner and Head of ICT.

This includes:

3.6 End-point management application: In October the Constabulary began the implementation of a new end-point management application. This application will provide greater analysis and transparency of the network, it's installed applications, removable devices in use, and will highlight many currently unknown vulnerabilities (such as unauthorised USB devices, out of date software versions, etc.)

3.7 The application will apply to all users and departments and will assist with implementing an agreed force standard across the endpoint estate. In some instances, it will require departments and individuals to change, alter, or cease locally or personally adopted practices (practices which may currently introduce risk or vulnerability.)

3.8 Cyber Audit: In January 2018, a Cyber-Threat audit will be carried out by Information Security and members of the ICT SMT. This will provide a dashboard and overview of its strengths and weaknesses and provide the opportunity to produce a continuing, graphical dashboard for the Chief Officer Group, and strategic direction for improvement within Information Security and ICT.

3.9 Cyber-Incident Response Retainer: In recognition of the level of specialist skills required in responding to a cyber-security incident, the Constabulary has entered into an annual Cyber Response Retainer with the NCC Group. This provides 24/7 support in terms of specialist advice, consultation, and if required, on-site support.

3.10 Table Top exercises: Preparations are underway to develop a series of table top exercises to test the response and readiness of staff and departments. The initial exercises will be carried out to test teams from within ICT. Further workshops will then be developed to incorporate other departments and Gold Command. This will also allow for a comprehensive gap analysis to be undertaken

3.11 It is accepted that staff and senior managers can be both an organisations greatest weakness and also its greatest strength. Under the direction of the Information Governance Board the Constabulary intends to address the balance. Work is currently underway by the

Records Manager and Information Assurance Manager to deliver a comprehensive series of training to all its Information Asset Owners.

3.12 In support of this over the next 12-months an audit of all the Constabulary's major system will be undertaken and a formal risk assessment produced; to inform both the Asset owners and Senior Management

3.13 *A training and awareness programme* is being developed for all users within the Constabulary. This is currently in its infancy but will be delivered during 2018

3.14 ICT resources – recruitment is currently underway for a new dedicated "Essential Infrastructure Maintenance" team within ICT. This team will be ring-fenced from project work and will be responsible for ensuring the infrastructure is properly managed, patched, maintained, and kept in line with force and national requirements; working closely with Information Security. This will address some resourcing constraints which are currently hindering ICT's capacity to undertake some of the regular, but essential, security based tasks.

4 Implications

Financial:	All identified costs are managed within existing budgetary constraints
Legal:	None
Equality Impact Assessment:	Not applicable
Risks and Impact:	Low
Link to Police and Crime Plan:	Not applicable

5 List of attachments / appendices

- None

6 Background Papers

- None