DIGITAL INNOVATION AND EFFICIENCY COMMITTEE

Item No……

Report title:	**Cyber Security Update**
Date of meeting:	**23 January 2019**
Responsible Chief Officer:	**Executive Directors of Finance and Commercial Services and Strategy and Governance**
Strategic impact: Cyber-attacks and the risk of cyber-crime against Norfolk County Council continues to increase and so it is essential that the Council's ability to protect itself from these attacks and to minimise the impact of any breach is continuously improved.	

Executive summary

The Authority commissioned an expert independent Cyber Security Audit in 2017. This paper provides an update of the subsequent actions that we are undertaking to improve the Authority's Cyber Security position.

In September 2017 the Cyber Security Audit findings were reported to this committee; the Audit found the Authority's Cyber Security posture was "Good" with 25 recommendations providing opportunities to move the Authority to "Excellent".

Cyber Security threats continue to grow in frequency and complexity

50% of the "High Priority" recommendations have been completed

80% of the remaining "High Priority" recommendations will be completed by Q2 2019

40% of the "Medium and Low" Priority recommendations have been completed

Recommendations:

1. **To note the information provided in this report and the importance of ongoing investment in the continuous improvement of our cyber security capabilities.**

1. Background

1.1 In May 2017 the Authority commissioned Silverthorn Ltd to complete an independent Cyber Security Audit of the ICT facilities.

1.2 The Audit found the Authority's Cyber Security posture was "Good" with 25 recommendations providing opportunities to move the Authority to "Excellent".

2. Progress

2.1 High Priority recommendations – 50% completed. Completed actions:

ID	Recommendation	Closing Actions
9 & 16	Ensure there is a formal process and responsibility as part of the Security Incident and Event Management (SIEM) system, and we recommend reviewing what is currently monitored and deploy the SIEM system to monitor internal servers.	Formal operation process designed and implemented; identified and added missing critical systems
10	Proactive monitoring of network logs must be a daily activity of the Network Team	Daily monitoring process designed and added to SIEM management processes
11	RACI approach be used across all of these areas as the biggest single improvement to NCCs Cyber Risk and threat profile will be through closer integrated working between ICT on the technical side and Information Management on the information governance and risk side.	RACI matrix and responsibilities have been generated and approved
17	Put a robust SIEM policy and regime in place, this needs to cover at a minimum the logs and configurations for; · Website · Firewalls · Proxy Servers (Including Digital Certificates) · VPN Servers · Wifi (Radius) servers · Mail Servers · Active Directory · Key Routers, bridges and switches	SIEM Policy has been developed and implemented. Listed configuration items have been added where not already monitored by SIEM system

2.2 Outstanding High Priority Recommendations:

ID	Recommendation	Progress & Expected Close Date
15	Review the SIEM platform. It may be more cost effective to renew/replace the existing appliance with a software / cloud solution from the same or different supplier.	Contract for new SIEM platform awarded 2nd Jan 2019, implementation expected by March 2019.
18	We recommend regular patching of all web services. All web applications pen	RACI responsibilities completed; developing

	tested before they go live. Web services to be scanned quarterly to ensure all patches are applied. SIEM monitoring to be proactive and near real time	cost justification to enable onsite security testing capability; review of procurement processes to ensure testing is included in future procurements. September 2019
19	A good SIEM and pro-active web monitoring and response process can mitigate a lot of issues. The OWASP controls will help here. If NCC moves to a full cloud service, then these protections and monitoring can be built in as part of the core (either Amazon Web Services or Microsoft Azure), for instance.	All web services have been added to SIEM monitoring. OWASP review of controls within Web development environment due for completion March 2019
21	We recommend NCC check their Office 365 configurations against the NCSC (CESG) Guidance.	Initial review complete, generation 2 work packages; 1 complete, 1 scheduled for completion by March 2019
23	Define and update the whole Incident Management and Incident response process. This should include the policy, forms, quantifying the incident levels and impacts	Template developed based on industry best practice, circulation & signoff scheduled March 2019.

2.3 Of the 12 Medium Priority recommendations, 4 have been completed and 8 remain open.

2.4 Of the 3 Low Priority recommendations, 2 have been completed and 1 remains open.

3. Other Cyber Security Improvements

3.1 One of the most critical aspects of improving Cyber Security is the education and training of users, to ensure they practice good cyber hygiene and are informed enough to identify Cyber Security risks

3.2 A major program of training and education will be provided to all Norfolk County Council users and Members from Q2 2019 to increase Cyber Security awareness and skills

3.3 A significant investment has been made in Microsoft products this year to improve cloud security of the Office 365 service to further reduce the risk of a Cyber Security Breach.

4. Financial implications

4.1 There are no significant financial implications arising from this report. The IMT budget includes sufficient allocated funds to carry out and maintain the improvements described in this report.

5 Issues, risks and innovation

5.1 There are no significant issues arising from this report. All identified improvements will be made as identified in the original audit and IMT officers will continue to work with external expert's agencies, individuals and our network of peers and vendors to ensure we continuously assess cyber risks and seek innovative solutions for ongoing improvement.

Officer Contact

If you have any questions about matters contained in this paper, please get in touch with:

Officer Name:	**Tel No:**	**Email address**:
Andy Ambridge	01603 973115	andy.ambridge@norfolk.gov.uk

If you need this report in large print, audio, Braille, alternative format or in a different language please contact 0344 800 8020 or 0344 800 8011 (textphone) and we will do our best to help.

•