APPENDIX 1 - Schools' cyber security advice CISO, Ealing Council.

This is intended to advise on the areas that could be tested or verified by the schools directly or their IT support company. The results should be verified by production of test results for review and action by the internal IT support function or attestation from the school's support company that they have been carried out and any issues rectified.

This note is not intended to replace industry good practice or specific guidance provided by central government. Some useful links are attached below.

End-point assessment (EPA) qualification level guidance - GOV.UK (www.gov.uk)

Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

Cyber crime and cyber security: a guide for education providers - GOV.UK (www.gov.uk)

The suggested testing is broken down into target areas and by suggested essential and 'recommended minimum' testing. This is because it is appreciated that budgetary constraints may be an issue.

While we recognise that a risk-based approach must be considered on balance along with costs. The costs of rectifying a significant event could run to 5 or 6 figures and cause significant disruption to a school including closure.

However, the advice is to conduct at least the 'recommended minimum' testing in each section and to consider proposals more than these, that are tailored by a cyber company for your specific circumstances. I have included a note to indicate the advantages and disadvantages in each area.

The scanning is laid out in order of increasing effectiveness and cost. Schools should give serious consideration to mandatory cyber security awareness training for staff and pupils.

Essential testing

A yearly vulnerability scan should be conducted on the external IP addresses and URLs used by the school, using industry-leading tools such as 'Nessus'. This will identify security issues with the external interfaces of the school and recommend actions to be followed.

A yearly vulnerability scan should be conducted on the internal IP addresses, including the server, network and desktop estate used by the school, using tools such as 'Nessus'. This will identify security issues internal to the school and recommend actions to be followed.

Advantage –

1. This will identify areas of concern and remediation actions to secure the perimeter.

Disadvantages –

1. This is a point in time and things move very fast in IT security and the results can be quickly out of date.
2. It can create a false sense of security.

Recommended minimum testing

A monthly vulnerability scan should be conducted on the external IP addresses and URLs used by the school, using tools such as 'Nessus'. This will identify security issues with the external interfaces of the school and recommend actions to be followed.

A monthly vulnerability scan should be conducted on the internal IP addresses, including the server, network and desktop estate used by the school, using tools such as 'Nessus'. This will identify security issues internal to the school and recommend actions to be followed.

Advantages –

1. This will identify areas of concern and remediation actions to secure the perimeter.
2. It is more in line with manufacturers monthly security patching cycle.
3. The rectification works drive good practice.

Disadvantage –

1. There may be additional work to be covered, to address vulnerabilities and recommended actions.
2. It may increase IT costs to ensure both core business and security are covered.

Additional testing.

The Council would additionally recommend a yearly internal penetration test assessment, this would test the schools' defences against active attack by a criminal/hacker. This would include an internal vulnerability assessment, network, and device configuration reviews, and build reviews. This allows an active audit of the security work of the IT support function and can form the basis of a 'service improvement plan' for security.

The Council due to its position conducts **constant** testing and monitoring of its estate including all the above items. It also hunts for threats to the organisation from 'criminals/hackers on the internet and dark web.

Any questions please email me on griffink@ealing.gov.uk