Dear Colleagues

I am writing to you as the Chief Information Security Officer for the Department for Education.

We have been working closely with the National Cyber Security Centre (NCSC) and have been made aware of an increasing number of cyber-attacks involving ransomware infections affecting the education sector recently, notably multi-academy trusts. These incidents appear to be financially driven but opportunistic, taking advantage of system weaknesses such as unpatched software, poor authentication systems or the susceptibility of users to misdirection.

Following our advisory which we sent via the Covid-19 Daily Email on the 22 March, I am keen to support you in taking appropriate actions to protect your institutions, especially when backing up the vital data for your institutions.

It is important that as heads of multi-academy trusts you understand the nature of the threat and the potential for ransomware to cause considerable damage to your institutions in terms of lost data and access to critical services, as highlighted in the NCSC Alert. Especially at a time where there is a heavy reliance on technology, additional reporting and a change in the nature of examinations. We are aware of the increased burden on you at this time but keen to ensure that MATs are protecting themselves.

The information we sent to you included a mention on cyber security preparedness. Part of this is managing your key risks, identifying your ‘crown jewels’ and ensuring you have an incident action plan, along with your defences. Having the ability to restore the systems and recover data from backups is vital in the event of an incident. You should ask your IT team or provider to confirm that:

- they are backing up the right data – for this year there are additional areas to consider including Covid-19 testing information and associated data, data relating to exams this year and alongside other key elements. Backups should be done on a regular basis.
- the backups are held offline – fully offline and not connected to your systems or in cold storage, following the 3-2-1 rule ideally (see advice below on offline backups)
- backups are tested appropriately – not only should you ensure backups are done regularly you should ensure that they have been tested to ensure you can restore services and recover data from the backups

Please get in touch with us at Sector.SECURITYENQUIRIES@education.gov.uk to confirm that you are taking action to protect your systems and ensure that you have both a backup regime and incident management plan in place.

Please note that we are working with NCSC on a webinar for schools on ransomware, this will be held during CYBERUK Online in May 2021, we will advertise with further details.

Finally, we must remind you of the Department for Education's stance on ransomware payments. The DfE supports the National Crime Agency's recommendations not to encourage, endorse, or condone the payment of ransom demands. Payment of ransoms has no guarantee of restoring access or services and will likely result in repeat incidents to educational settings.

Kind regards,

Jon Gilbert
Chief Information Security Officer
Department for Education

Additional sources of information

For ease of reference, we have included a number of useful links relating to cyber security:

1. NCSC Alert on the current cases of ransomware
2. Ransomware advice and guidance for your IT teams to implement
3. Offline backups in an online world
4. Backing up your data
5. Practical resources to help improve your cyber security
6. School staff offered training to help shore up cyber defences – NCSC.GOV.UK

Reporting cyber incidents:

1. Enact your incident management plan
2. Contact the NCSC
3. Contact your local law enforcement and Action Fraud
4. Inform the Department for Education by emailing: sector.securityenquiries@education.gov.uk