Risk Protection Arrangement - Cyber Guidance

Introduction

In response to member demand, the RPA is including cover for **Cyber Incidents** as standard from 2022/23 membership years. Cyber was ranked #2[1] in a survey in May 2020 of the additional covers that members would most like to see introduced. In April 2021, we launched a 12-month Cyber pilot with over 600 member schools to gain a better understanding of their cyber standards and level of maturity, which has helped us determine the scope of the new cover and develop advice, information, and guidance to support school resilience.

A Cyber Incident is defined in the RPA Membership Rules as:

"Any actual or suspected unauthorised access to any computer, other computing and electronic equipment linked to computer hardware, electronic data processing equipment, microchips or computer installation that processes, stores, transmits, retrieves or receives data."

Your RPA cover includes a 24/7 dedicated helpline **0800 368 6378** and a dedicated email address **RPAresponse@CyberClan.com** available to you in the event of a Cyber Incident.

To be eligible for RPA Cyber cover, there are 4 conditions that members must meet:

1. Have offline backups. Help and guidance on backing up is available from the National Cyber Security Centre (NCSC) and should ideally follow the 3-2-1 rule explained in the NCSC blog Offline backups in an online world - NCSC.GOV.UK

   It is vital that all education providers take the necessary steps to protect their networks from cyber-attacks and have the ability to restore systems and recover data from backups. Education providers should ask their IT teams or external IT providers to ensure the following:

   a) Backing up the right data. Ensuring the right data is backed up is paramount. Review all the data assets your school has access to and decide which are critical and how long you would be able to function without each one.

   b) Backups are held fully offline and not connected to systems or in cold storage, ideally following the 3-2-1 rule explained in the NCSC blog Offline backups in an online world: https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world

   c) Backups are tested appropriately, not only should backups be done regularly but need to be tested to ensure that services can be restored, and data recovered from backups.

   Further Help and guidance on backing up can be found at: Step 1 - Backing up your data - NCSC.GOV.UK. https://www.ncsc.gov.uk/collection/small-business-guide/backing-your-data

[1] #1 was Motor cover. The RPA has carried out a public consultation and is planning to conduct a survey to gather in-depth data on members current motor insurance arrangements.

There is also a useful NCSC presentation on YouTube with more details on offline backups: Building Resilience: Ransomware, the risk to schools and ways to prevent it

2. All Employees or Governors who have access to the Member's information technology system must undertake NCSC Cyber Security Training by the 31 May 2022 for local authority maintained schools or by 1 September 2022 for academy members. Upon completion of the NCSC Cyber training video, the certificate website address will need to be manually entered into the search bar. The certificate can then be downloaded or printed and the name of the participant added. Alternatively, the training can be completed through the PowerPoint slides available and click on the link at the end of the presentation to access the certificate. In the event of a claim the Member will be required to provide the certificates as evidence.

3. Register with Police CyberAlarm. Registering will connect Members with their local police cyber protect team and in the majority of cases, a cyber-alarm software tool can be installed for free to monitor cyber activity. Where installed the tool will record traffic on the network without risk to personal data. When registering HERE, use the code "RPA Member" in the Signup code box beneath your contact details.

4. Have a Cyber Response Plan in place. A template is available for you to use to draft a school-specific plan if you do not already have one. It can be downloaded from the RPA Information & Documents page on the TopMark Claims Management website, from the RPA members portal or by emailing RPA.DFE@education.gov.uk

For full terms and conditions of Cyber cover, please refer to the relevant Membership Rules on gov.uk.

Helping your school to be prepared

It is vital education providers regularly review their existing defences and take the necessary steps to protect their networks. In addition to the 4 conditions of cover detailed above, there are several suggested measures that schools can implement to help themselves to improve their IT security and mitigate the risk of a cyber-attack:

- Regularly review IT Security Policy and Data Protection Policy.
- Assess the school's current security measures against Cyber Essentials requirements, such as firewall rules, malware protection, and role based user access. Cyber Essentials is a government-backed baseline standard, which we would encourage all RPA members to strive towards achieving wherever possible.
- Ensure Multi-Factor Authentication (MFA) is in place: A method of confirming a user's identity by using a combination of two or more different factors.
- Implement a regular patching regime: Routinely install security and system updates and a regular patching regime to ensure any internet-facing device is not susceptible to an exploit. This includes Exchange servers, web servers, SQL servers, VPN devices and Firewall devices. Ensure that security patches are checked for and applied on a regular basis. Vulnerabilities within Microsoft Exchange Servers have been the root cause of many cyber-attacks in the last six months. It is highly recommended that on-premises exchange servers are reviewed and patched/updated as a high priority and moving to an Office 365 environment with MFA if possible.

- Enable and review Remote Device Protocols (RDP) access policies: The use of external RDP access to a device is not recommended and allows attackers to brute-force access to any device that is externally accessible. Mitigating measures are:
    - If external RDP connections are used, MFA should be used
    - Restricting access via the firewall to RDP enabled machines to allow only those who are allowed to connect
    - Enable an account lockout policy for failed attempts
    - The use of a VPN tunnel to access a network in the first instance, and then allowing users to subsequently use RDP or RDS to access a device afterwards is highly recommended
- Review NCSC advice regarding measures for IT teams to implement: Mitigating malware and ransomware attacks - NCSC.GOV.UK
- Provide awareness training for staff to recognise, report, and appropriately respond to security messages and/or suspicious activities.

Further advice and guidance

- **The NCSC website has an extensive range of practical resources to help improve Cyber Security for Schools - NCSC.GOV.UK**

Actions in the event of an incident

If you suspect you have been the victim of a ransomware or other cyber incident, you should take the following steps immediately:

- Enact your **Cyber Response Plan**
- Contact the 24/7/365 RPA Cyber Emergency Assistance:
    - By telephone: **0800 368 6378** or by email: **RPAresponse@CyberClan.com**
    - You will receive a guaranteed response within 15 minutes
    - Incident information will be recorded, advice will be provided and any critical ongoing incidents will be contained where possible
    - Subject to the claim being determined as valid, an expert Incident Response team will be deployed to rapidly respond to the incident, providing Incident Response services including: forensic investigation services and support in bringing IT operations securely back up and running.
- Inform NCSC - https://report.ncsc.gov.uk
- Contact your local police via Action Fraud Action Fraud website or call **0300 123 2040**
- If you are a part of a Local Authority (LA), they should be contacted
- Contact your Data Protection Officer
- Consider whether reporting to the ICO is necessary report at www.ico.org.uk **0303 123 1112**
- Contact the Sector Security Enquiries Team at the Department for Education by emailing: sector.securityenquiries@education.gov.uk

Please be aware that speed is of critical importance during a cyber incident to help protect and recover any systems that may have been affected and help prevent further spread.

For any further help or guidance about RPA Cyber Cover, email RPA.DFE@education.gov.uk