Acronis Cybersecurity in Education

Introduction

Acronis provides schools with comprehensive cyber protection that helps them comply with the guidance from the Department for Education (DfE) and the National Cyber Security Centre (NCSC), addressing the threat posed by ransomware.

NCSC guidance focuses on much more than just backup. Here's a detailed explanation of how Acronis helps schools comply with the NCSC's 10 steps to Cyber Security, which is in turn referenced by the DfE.

Backup

NCSC guidance states that organisations should:

1. Make regular backups of important files and test the restoration process to ensure it works properly
2. Create offline backups stored in a separate location (3-2-1 backup rule)
3. Have multiple copies of files stored in different backup solutions and storage locations
4. Choose a cloud service that protects previous versions of backups and allows for easy restoration. This prevents both live and backup data from becoming inaccessible
5. Connect backups only to known clean devices before initiating the recovery process
6. Scan backups for malware before restoring files
7. Regularly patch endpoints to prevent exploitation of known vulnerabilities by attackers

Acronis easily meets all these requirements as standard and includes additional protection such as immutability.

Ransomware active protection

Acronis includes advanced anti-ransomware technology that proactively detects and blocks ransomware attacks, preventing them from encrypting school data. If ransomware successfully infects any files, organisations can successfully roll back to before the infection occurred. Thanks to full integration with Acronis' backup technology, this can be achieved in seconds, with a single click, minimising the impact of the attack. This technology is included free of charge.

Immutability

Backup immutability ensures that you can access deleted backups during a specified retention period. You can recover content from these backups, but you cannot change, move or delete them. When the retention period ends, the deleted backups are permanently erased. The default retention period is 14 days, but you can specify any period within the range of 14 to 365 days.

If a whole company is deleted in error or malice, the account, all users, data and services can be recovered in the same way as backups. The retention period for this protection is 30 days.

Asset management

Acronis assists with asset management in line with NCSC guidance, enabling organisations to:

1. Identify critical assets and prioritise their protection
2. Maintain an inventory of hardware and software
3. Integrate asset management into security activities
4. Streamline the approach to asset management

Patch management

Acronis includes patch management capabilities that enable schools to keep their systems and software up to date with the latest security patches, in line with NCSC guidance (below):

1. Establish a patch management policy
2. Identify and prioritise vulnerabilities
3. Test patches before deployment
4. Develop a patch deployment strategy
5. Keep software up to date
6. Automate patch management
7. Monitor patching effectiveness

This helps prevent vulnerabilities that ransomware attackers often exploit.

Centralised management

Acronis Cyber Protect Cloud provides a centralised management console that allows schools to monitor and manage their cybersecurity measures from a single interface. This simplifies the management of security policies and ensures consistent protection across all devices and systems.

Vulnerability management

Acronis Cyber Protect Cloud helps schools establish a vulnerability management process, including automated vulnerability scanning capabilities that help schools detect and respond to ransomware attacks in real time. Schools can triage vulnerabilities based on severity and prioritise their remediation efforts. This helps reduce the likelihood of systems being exploited by ransomware.

User education and awareness

Acronis, through its partnership with the North East Business Resilience Centre (NEBRC), offers a valuable opportunity for schools to enhance the digital literacy and cybersecurity awareness of their staff. The NEBRC equip school staff with the necessary skills to navigate the ever-evolving digital landscape - confidently and securely. This partnership not only strengthens the cybersecurity posture of schools but also fosters an environment of continuous learning and adaptation to technological advancements. Learn more about the NEBRC here.

Endpoint protection

Acronis provides endpoint protection to secure school devices, including computers, laptops, and mobile devices. This includes anti-malware, anti-phishing, and web filtering capabilities to prevent malicious attacks. By also securing devices used for home and mobile working, schools can further mitigate the risk of ransomware attacks.

Incident management

Acronis Cyber Protect Cloud helps schools develop an effective incident response plan. It provides tools for incident detection, containment and recovery. Schools can define incident response procedures and automate response actions to minimise the impact of ransomware attacks.

Summary

By implementing Acronis Cyber Protect Cloud, schools can enhance their cybersecurity posture, comply with DfE and NCSC guidance and effectively protect their data from ransomware attacks. Acronis provides a comprehensive set of tools and features that help address the NCSC's 10 steps to Cyber Security, helping schools establish a robust cybersecurity framework.

Simplify your cyber resilience today

Acronis Cyber Protect Cloud is the integrated platform that unites backup and next-generation, MI-based anti-malware, antivirus, and endpoint protection management in one solution.

TRY NOW

Acronis

Learn more at
acronis.com