Information Security Policy

Ransomware Policy

1. Introduction

Ransomware attacks on the education sector have been increasing since early 2021. The NCSC (National Cyber Security Centre) have published guidance and practical resources to help schools minimise the opportunity for such attacks to occur. The main vectors for increasing cyber-attack vulnerability are:

- Remote access – weak passwords, lack of multi factor authentication and unpatched vulnerabilities
- Remote Desktop Protocol – user credentials gathered through data breaches, phishing or credential harvesting.
- Phishing
- Other vulnerable hardware of software

2. Purpose

This is an internal policy that defines how Chelmsford County High School for Girls (CCHS) prepares to defend against the threat of ransomware attacks on the school's computer systems. The policy defines processes and procedures that aim to reduce the risk of exploitation by ransomware attacks, to lessen the impact and to recover from an incident quickly and safely.

3. Responsibilities

All employees with direct access to the CCHS information technology systems are expected to conform to this policy.

CCHS's IT team are responsible for providing support in complying with this policy.

The IT Manager is responsible for ensuring that this policy is annually reviewed and that changes are made in the event of legislation change or compliance frameworks such as the Cyber Essentials scheme are updated.

4. Definition

The National Cyber Security Centre's (NCSC) definition reads: *"Ransomware is a type of malware that prevents you from accessing your computer (or the data that is stored on it). The computer itself may become locked, or the data on it might be stolen, deleted or encrypted."*

5. Preparation

CCHS recognises and acknowledges the threat of ransomware attacks and the severity of the impact on the CCHS's computer systems and operations and aims to prepare accordingly. To prepare for and defend against ransomware attacks, CCHS deploys strategies and controls which may include the following:

Ransomware Policy

- **Data classification** - Not all data is equal and thus data should be classified and stored according to the sensitivity level. The school should be aware of the systems that process and store critical/sensitive data and such must be documented.
- **Effective backup strategies** - Backup systems are the first port of call in the case of a ransomware attack. Ransomware attacks aim to sabotage recovery operations thus, the school aims to implement effective backup strategies and data recovery operations by:
    - conducting regular backups of data, and most importantly, of critical/sensitive data
    - having offline backups preferably offsite
    - having multiple copies of the same file using different backup systems
    - scanning backup systems for malware where possible, especially before recovery
    - regularly testing data recovery operations
- **Staff awareness training** - The school conducts regular staff awareness training to educate staff in areas which include but not limited to best security practices, common attack vectors, phishing email attacks, password handling, reporting channels.
- **Patch management** - CCHS follows the patching schedule described in CCHS's Patch Management Policy to reduce an attacker's probability of gaining access through a discovered security vulnerability.
- **Cyber insurance** - Cyber insurance will assist CCHS with recovery costs in the case the School suffers a breach.
- **Regular incident management plan rehearsal** - A timely and well-coordinated response to a ransomware attack might lessen the impact. CCHS aims to regularly review and test the incident management plan to ensure that it's up-to-date and that all the pre-defined roles and responsibilities are clearly defined.

6. 5. Monitoring and Detection Controls

Network monitoring strategies and suspicious behaviour detection controls are implemented across CCHS's computer systems and networks. This approach aims to implement technology best practices as well as non-technical approaches which may include:

- Ensuring anti-malware software applications are installed and enabled on all endpoints, virus signature databases are always up-to-date and files are set to be scanned on-access.
- Automated suspicious/unusual behaviour event notifications including the deploying a monitored 'honeypot' folder at the top of critical data directories that serves as an early-warning.
- Deploying robust email filtering systems to block, quarantine or flag suspicious emails.
- Reporting of suspicious emails or events by school staff.

7. 6. Eradication and Recovery Process

In the case School is breached, the main aim is to contain the malware to prevent it from spreading to other systems. CCHS follows the NCSC guidelines to help limit the impact:

- Quick disconnection and isolation of infected computers, laptops or tablets from all network connections. If multiple devices are infected, network equipment including routers, switches and wireless access points may also need to be turned off.
- User credentials for user accounts associated with the infected device will be reset
- The latest patches will be applied to non-infected devices
- Infected devices are wiped and rebuilt

Ransomware Policy

- All backup systems must be thoroughly scanned for malware before data recovery operations are commenced.
- Verify that endpoint anti-malware software applications are installed, up-to-date and enabled on all systems.
- Continuous monitoring of network traffic and anti-malware scans to verify if traces of the malware still exist.

8. 7. Post Incident

Lessons learnt are discussed, documented and changes are made to the incident management plan and other internal processes where necessary.

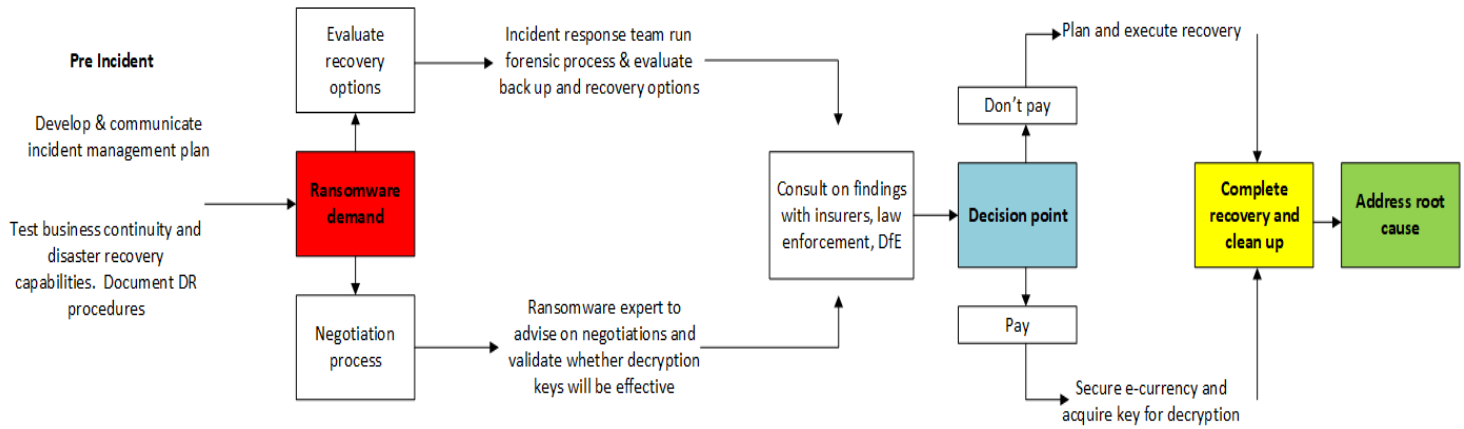
9. 8. Ransomware Payments

In the event that the CCHS's backup systems fail and data is unrecoverable, the only option might be to pay and that so being, CCHS follows the National Crime Agency (NCA) and the ESFA's guidance regarding ransomware payments.

In accordance with section 6.17 of the Academy Trust Handbook, CCHS will contact the ESFA first to obtain permission to pay any cyber ransom demands. The ESFA supports the National Crime Agency's recommendation not to encourage, endorse or condone the payment of ransom demands. CCHS is fully aware that by making such payments:

- our computer systems may be more likely to be targeted in the future
- there is no guarantee that the School's data will be returned
- the School will be paying cybercriminals which will likely be funding organised crime.

The Ransomware Decision Process is summarised below:



Information Security Policy

Ransomware Policy

Change Log

Version	Changes	Author	Change Date	Approval Date
0.1 – Draft 1.0 - Approved	First draft based on Secure Schools Ltd model policy and introduction / ransomware flow chart additions	Melissa Mulgrew	12th May 2022	22nd June 2022

Approved by	Facilities & Finance Committee
Date Approved	22nd June 2022
Date of Next Review	June 2023
Model Policy	Secure Schools Ltd