Ransomware and Data Protection Guidance

Information Governance (IG) Services.

Adopted January 2023

Reviewed January 2024

YourIG

Bringing Information Governance solutions to you.

Contents

Ransomware and Data Protection Guidance

Rationale

Personal data breaches from the ICO's caseload recently have seen a steady increase in the number and severity caused by ransomware. This is a type of malicious software or "malware" is designed to block access to computer systems, and the data held within them, using encryption.

This guidance presents eight scenarios about the most common ransomware compliance issues the ICO have seen.

What is ransomware?

Ransomware is a type of malware that attempts to unlawfully encrypt files on a host computer system.

A ransomware attack occurs when an attacker gains access to the school computer systems and delivers malicious software into the network. This software, or 'payload,' then makes the data unavailable through encryption or deletion. Ransomware is often designed to spread from device to device to maximise the number of files it can encrypt.

The 'ransom' element comes from the ransom note left by the attacker requesting payment in return for restoring the data. This is usually done by a decryption key that only the attacker can access.

Where personal data is encrypted as the result of a ransomware attack, this constitutes a personal data breach because the school has lost timely access to the data.

Unless the school has a backup of the data, the school will not usually be able to recover it unless it decides to comply with the attacker's demand for payment. Even if the school decides to pay the ransom fee, there is no guarantee that the attacker will supply the key to allow the school to decrypt the files.

Why is ransomware an important data protection topic?

In recent years, ransomware attacks are one of the most common cyber incidents affecting personal data. The attack can lead to the loss of timely access to personal data. Permanent data loss can also occur, if appropriate backups are not in place.

The National Cyber Security Centre (NCSC) recognises ransomware as the biggest cyber threat facing the United Kingdom. The most recent threat landscape report from the European Union Agency for Cyber Security (ENISA) has also assessed ransomware as the prime threat with cybercriminals increasingly motivated by monetisation.

The attacks are becoming increasingly damaging and this trend is likely to continue.

Malicious and criminal actors are finding new ways to pressure organisations to pay. For example, through uploading a copy of the data and threatening to publish it.

Sectors such as education, health, legal services and business are amongst the most targeted.

Scenarios about the most common ransomware compliance issues?

The eight scenarios about the most common ransomware compliance issues the ICO have seen are as follows:

Scenario 1 Attacker Sophistication: 'Scatter gun' style attacks are a common attack method. This type of attack is indiscriminate and does not have a specific target. For example, the attacker may send thousands of phishing emails attempting to deliver ransomware to at least one victim, whoever that may be.

Scenario 2 Data Breach: If a school is subject to a cyber-attack, such as ransomware, the school is responsible for determining if the incident has led to a personal data breach.

Scenario 3 Breach Notification: The school is required to notify the ICO of a personal data breach no later than 72 hours after having become aware of it unless the breach is unlikely to result in a risk to the rights and freedoms of individuals.

Scenario 4 Law Enforcement: If the school has been subjected to a ransomware attack it is recommended that they contact law enforcement such as the Police or The National Cyber Security Centre.

Scenario 5 Attacker tactics, techniques and procedures: Tactics, techniques and procedures (TTPs) describe the methods attackers use to compromise data. These can include phishing, remote access, privileged account compromise, and known software or application vulnerabilities.

Scenario 6 Disaster Recovery: Backup of personal data is an important control mitigating the risk of ransomware. However, it is common that attackers will attempt to either delete or encrypt the backup. Schools should consider their current backup strategy. Performing a threat analysis against the backup solution and considering how an attacker could delete or encrypt the data is recommended.

Scenario 7 Ransomware Payment: Law enforcement do not encourage, endorse, nor condone the payment of ransom demands. The ICO supports this position.

Scenario 8 Testing and assessing security controls: The UK GDPR requires schools to regularly test, assess and evaluate the effectiveness of the technical and organisational controls using appropriate measures. These measures may include breach notification, account management, patch management, attack tactics, techniques and procedure, audit, and disaster recovery.

Additional Guidance

This can be found via the following links:

Ransomware and Data Protection Guidance

The National Cyber Security Centre (NCSC)