Ransomware and data protection compliance

At a glance

- Personal data breaches from the ICO's caseload during 2020/2021 have seen a steady increase in the number and severity caused by ransomware. This is a type of malicious software or "malware" designed to block access to computer systems, and the data held within them, using encryption.
- Ransomware is a type of malware that attempts to unlawfully encrypt files on a host computer system.
- This guidance presents eight scenarios about the most common ransomware compliance issues we have seen.

Checklist

Governance

☐ We establish and communicate a set of suitable security policies that provide direction to appropriate levels of security.

Asset identification

☐ We identify, document and classify the personal data we process and the assets that process it. Examples of personal data that typically require a higher classification level include large volumes of data, children's data and special category data.

Technical control selection

☐ We determine and document appropriate controls to protect the personal data we process. We use the NCSC Mitigating Malware and Ransomware guidance to give us a set of practical controls we can implement to prevent ransomware.

Access controls

☐ We implement appropriately strong access controls for systems that process personal data. For internet facing services, such as remote access solutions, we enable multi-factor authentication or other alternatively strong access controls.

Vulnerability management

☐ We implement a policy that defines our approach to patch management. We prioritise patches relating to internet-facing services, as well as critical and high risk patches. We use the NCSC Vulnerability management guidance to support us further.

Staff education and awareness

☐ We ensure all relevant staff have a baseline awareness of attacks such as phishing. We consider providing additional and specific security training for staff with responsibility for IT Infrastructure and security services.

Detection

☐ We implement appropriate controls to be able to detect and respond to an attack before it can exploit the personal data we process. If we are a smaller organisation, we use the NCSC Logging Made Easy solution to support us in developing basic enterprise logging capability.

Incident response

☐ We define an incident response plan that guides us in the event of a ransomware attack. We include thresholds for ICO and affected individual notifications.

☐ We perform regular tests of our plan, for example, the NCSC Exercise in a Box helps us practise our response in a safe environment.

Disaster recovery

☐ We have disaster recovery and business continuity plans to support us in restoring personal data in a timely manner. Measures such as offline backups or those described in the NCSC "Offline backups in an online world" blog are important to ensure we can restore personal data.

Assurance

☐ We test, assess and evaluate our control environment using measures such as audits, vulnerability scanning, penetration testing and accreditation against proven security standards such as NCSC Cyber Essentials and other relevant standards of good practice.

In brief

- What is ransomware?
- Why is ransomware an important data protection topic?
- What can we do to prevent ransomware?
  - Scenario 1: Attacker sophistication
  - Scenario 2: Personal data breach

- Scenario 3: Breach notification
- Scenario 4: Law enforcement
- Scenario 5: Attacker tactics, techniques and procedures
- Scenario 6: Disaster recovery
- Scenario 7: Ransomware payment
- Scenario 8: Testing and assessing security controls

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 an organisation's 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 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, that constitutes a personal data breach because you have lost timely access to the data.

Unless you have a backup of the data, you will not usually be able to recover it unless you decide to comply with the attacker's demand for payment. Even if you decide to pay the ransom fee, there is no guarantee that the attacker will supply the key to allow you 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 your data and threatening to publish it.

As criminal actors look for additional ways to exploit the captured data, the risks to individuals have increased, including:

- potential permanent personal data loss;
- potential loss of control over their personal data;
- being further targeted in social engineering style attacks using the breached data (eg phishing emails); and
- their personal data being further maliciously used by criminal actors (eg to facilitate identify and financial fraud).

Sectors such as education, health, legal services and business are amongst the most targeted. However, all UK businesses that process personal data are at risk. This is due to the low barriers to entry, such as by using ransomware-as-a-service and opportunistic attacks.

What can we do to prevent ransomware?

You should review our checklist above, as well as the following eight scenarios. These are the eight most common ransomware compliance issues we have identified, based on past personal data breaches.

Scenario 1: Attacker sophistication

I am a small organisation that is aware of the growing threat of ransomware. However, I don't think attackers will be interested in targeting me. If they do, how can I protect the personal data I process?

'Scatter gun' style attacks are a common attack method. This is a type of attack that 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.

The NCSC Cyber Essentials is designed to support you in preventing basic and common types of attacks. The measures they describe will help you apply appropriate security measures, which are a requirement of the UK GDPR.

For medium and larger organisations, maintaining good cyber security practices is essential to defend against ransomware attacks. Assessing your cyber security arrangements and capabilities against relevant good practice models can support you protect personal data from the threat of ransomware, such as:

- NCSC 10 Steps to Cyber Security;
- ISO27001 for Information Security; and
- NIST Cyber Security Framework.

The NCSC Mitigating Malware and Ransomware attacks also provides specific guidance that can support you in preventing such attacks.

Scenario 2: Personal data breach

We have been subjected to a ransomware attack, but personal data has not been uploaded from our systems to the attacker. If the data has not been removed does this mean a personal data breach has not occurred?

If you are subject to a cyber-attack, such as ransomware, you are responsible for determining if the incident has led to a personal data breach. This is your first step in deciding if you should notify the ICO about the incident.

The UK GDPR defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

Where personal data is taken it typically results in unauthorised disclosure or access to personal data and therefore is a type of personal data breach. However, it is not the only consideration you should make when determining if a personal data breach has occurred.

You may have lost timely access to the personal data, for example because the data has been encrypted. This is a type of personal data breach because you have lost "access to" personal data. Temporary loss of access is also a type of personal data breach. For example, if there is a period of time before you restore from backup.

Therefore, loss of access to personal data is as much of a personal data breach as a loss of confidentiality.

However, just because a personal data breach has occurred does not automatically mean you should notify the ICO. Scenario 3 deals with a common breach notification scenario.

Scenario 3: Breach notification

We have established a personal data breach has occurred, but data has not been exfiltrated, therefore there are no risk to individuals. Do we still need to notify the ICO?

You are required to notify the ICO of a personal data breach without undue delay and 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.

This means once you have established a personal data breach has occurred, you should undertake a formal risk assessment. This is to determine the risks to individuals and the likelihood of such risks occurring. If you determine the risks to be unlikely, you do not need to notify the ICO. However, you must keep a record of any personal data breaches, regardless of whether you are required to notify, together with the risk assessment undertaken.

Where data is uploaded from your systems to the attacker it can increase the risks to individuals. Therefore, you should take data exfiltration into account as part of your risk considerations. Appropriate logging can support you in determining if personal data is likely to have been exfiltrated. The NCSC blog post "What exactly should we be logging" can support you in deciding what logs to collect and retain.

Without appropriate logs you may not generate the evidence to allow you to make an informed decision. If you determine there is no evidence of data exfiltration, the ICO may ask you to demonstrate what logs and measures you used to make this decision.

However, whilst exfiltration is an important consideration it is not the only one you should make. You should consider the rights and freedoms of individuals in totality. For example:

- Does the lack of availability impact on any individual rights, such as right of access to the personal data?
- Have individuals lost control of their personal data?
- Can you restore the personal data in a timely manner? If not, what does this mean for individuals?
- To what degree was the personal data exposed to unauthorised actors and what are their likely motivations?
- How confident are you in your detection and monitoring controls – could you have detected personal data being uploaded if it had occurred? If you do not have appropriate logs to make an informed decision, it may be helpful to determine if the attacker had the means, motivation and opportunity to exfiltrate the data. You can then use this assessment to make a risk-based decision.

Further reading

The ICO's Personal data breach assessment tool can support you in identifying reportable personal data breaches.

Our guidance on personal data breaches can also further support you in assessing reportable personal data breaches.

Scenario 4: Law enforcement

A ransomware attack has breached the personal data we process. We are planning to notify individuals, however, law enforcement are currently collecting evidence as this was a criminal attack. They have requested we delay notifying individuals until they has completed this. How do I comply with my GDPR obligations whilst also cooperating with law enforcement?

If you have been subjected to a ransomware attack it is recommended you should contact law enforcement.

Law enforcement play a fundamental role in protecting individuals and the ICO work closely with these agencies in providing a multi-agency response to ransomware. Recitals 86 and 88 of the UK GDPR provide direction should law enforcement recommend delaying data subject notification:

Recital 86:

> Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities

Recital 88:

> Moreover, such rules and procedures should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach

However, law enforcement involvement does not automatically mean you should delay notifying individuals. Should law enforcement request a delay in a public notification, you should work closely with the ICO. This will allow us to work with you and law enforcement to assess the risk to the individuals under respective legislation.

Scenario 5: Attacker tactics, techniques and procedures

> We have recently seen an increase in phishing emails coming into our organisation and are looking at what measures we can put in place to mitigate this risk. Are there any other specific attacker tactics that the ICO commonly see in ransomware attacks?

Tactics, techniques and procedures (TTPs) describe the methods attackers use to compromise data. Different attacks will use different types of TTPs, for example phishing is a common TTP to trick someone into giving up their credentials.

However, attacker TTPs are constantly evolving, as described within scenario one of this report. A good baseline of controls will reduce the likelihood of being exploited by basic levels of attack, such as those described in the NCSC Cyber Essentials.

Frameworks are available, such as the Mitre ATT&CK that provide a knowledgebase of TTP based on real world observations. The framework outlines each stage of an attack and the common TTPs that are used. These are a great resource to support you in identifying if your controls are appropriate to resist known TTPs.

During 2020/2021, we identified four of the most common TTPs from ransomware casework. The following practical advice for each example will support you in implementing appropriate measures.

Phishing: Attackers typically use social engineering techniques to trick you into doing something. Phishing is a common method we've seen to either deliver ransomware by email or to trick you into revealing your username and password.

Your security strategy should include ensuring all relevant staff receive basic awareness training in identifying social engineering attacks. In addition, you should consider tailoring the measures in the NCSC Phishing Attack guidance to your own organisation.

Remote access: The most common entry point into a network was by the exploitation of remote access solutions. Attackers often scan the internet for open ports such as remote desktop protocol and use this as an initial entry point. If they can capture valid credentials (eg by phishing, password database dumps or password guessing through brute force), they can authenticate by the remote access solution.

You should risk assess and document your remote access solution and identify appropriate measures in response to the risks. An access control policy that directs you to the minimum levels of controls required will support you in applying appropriate measures.

You should not use single-factor authentication on internet facing services, such as remote access, if it can lead to access to personal data. Use multi-factor authentication, or other comparably secure access controls.

The NCSC device security guidance provides further advice on designing a remote access architecture for enterprise services.

Privileged account compromise: Once an attacker has a foothold in the network it is common that they compromise a privileged account, such as a domain administrator account. This is typically done by either

- compromising weak passwords of privileged accounts;
- compromising service accounts that do not belong to a particular user;
- using well known tools to extract plain text domain administrator passwords, password hashes or Kerberos tickets from the host; or
- exploiting a known software or application vulnerability which has a patch available to fix it.

Once an attacker can elevate their privileges to a domain administrative level account they are typically in a commanding position and will usually deploy the ransomware through the domain controller.

The security of privileged accounts should be a high priority for you. Basic account hygiene can support you in protecting these accounts, such as:

- regular reviews of permissions;
- following the principle of least privilege;
- risk assessments of membership into privileged groups; and
- senior level approval of privileged group membership.

Further reading

The NCSC has a selection of guidance available that can further support you in identifying appropriate measures to protect privileged accounts.

- How to do secure system administration
- Protecting system administration with PAM

Known software or application vulnerabilities: The exploitation of known vulnerabilities where patches were available to fix the issue is a common method used by attackers. This was much more common than zero-day attacks where the vulnerability exploited is not yet publicly known and is typically crafted by advanced levels of attackers. In particular, attackers often scan, sometimes indiscriminately, for known vulnerabilities present in internet-facing device and services.

The NCSC vulnerability management guidance will support you in managing vulnerabilities within your estate.

Considering the following will also support you in managing known vulnerabilities:

- Identify the assets within your organisation, including the software and application you use.
- Define and direct your approach to the patch management lifecycle, including the process of identifying, assessing, acquiring, testing, deploying and validating patches.
- Maintain software and applications that are in support by the vendor.
- Identify vulnerabilities within your estate for both internal and external hardware and software (eg vulnerability scanning).

Scenario 6: Disaster recovery

We understand the UK GDPR requires appropriate controls to be able to restore personal data in the event of a disaster. We currently backup our data so we are able to restore it in the event of a ransomware attack. Is there anything else we should consider?

A ransomware attack can be amongst the most stressful times for an organisation. Planning for such an event is critical in ensuring you have the measures in place to be able to appropriately respond to it.

For smaller and medium sized organisations the NCSC Small Business Guide Response and Recovery gives you practical advice that will help you plan for dealing with an incident such as a ransomware attack.

For larger organisations the NCSC Incident Management guidance within its 10 steps to cyber security can support you in implementing appropriate controls.

A backup of your personal data is one of the most important controls in mitigating the risk of ransomware. However, it is common that attackers will attempt to either delete or encrypt your backup. You should therefore consider if your current backup strategy could be at risk. Performing a threat analysis against your backup solution and considering how an attacker could delete or encrypt the data is recommended. The questions below will help you get started in your threat assessment:

- Is your backup segregated or offline?
- What would an attacker need to compromise to gain access to the backup? For example, what accounts can access the backup? What accounts can perform deletion or edit the backups? How could an attacker compromise these accounts? How do you protect accounts that can access the backups?
- Are you able to detect changes to your backup? For example, if an attacker initiated a deletion of your backup, could you detect this?
- What device or IP address or both can access the backup repository? Can this be spoofed? Can an attacker access the device or repository that stores the backup?
- How would you respond if an attacker deleted or encrypted your backup?

Using your threat analyses will help you identify controls to mitigate the risks. Offline backups that are completely offline from the main network are one of the most secure ways to prevent attackers from accessing it. If you are using cloud backups, you should read the NCSC blog posts about protecting these backups Offline Backups in on online world and Cloud Backup options for mitigating the risk of ransomware.

Scenario 7: Ransomware payment

The attacker has provided a ransomware note saying it can restore the data if we pay the ransom fee. The attacker has also stated that if we pay they will not publish the data, so we are also considering if this would further reduce risk to individuals.

Does the ICO recommend the payment of the ransom to restore the data and mitigate risks to individuals?

Before paying the ransom, you should take into account that you are dealing with criminal and malicious actors. Even if you pay, there is no guarantee that they will provide you with the decryption key. "Double extortion" is also common, where you pay for the decryption key and the attacker then requires an additional payment to stop the publication of the data. Attack groups may also target you again in the future if you have shown willingness to pay.

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

You should also consider the terminology within the UK GDPR. It requires you to implement "appropriate measures" to restore the data in the event of a disaster. The ICO does not consider the payment of a ransom as an "appropriate measure" to restore personal data.

Appropriate measures include threat assessments, risk assessments and controls such as offline and segregated backups. If you can demonstrate appropriate measures in accordance with the state of the art, cost and risk of processing then you will be able to demonstrate "appropriate measures" and comply with those aspects of the UK GDPR.

If attackers have exfiltrated the personal data, then you have effectively lost control over that data. This means individuals have lost the protections and rights provided by the UK GDPR. For example, transparency of processing or subject access rights. For this reason, we do not view the payment of the ransom as an effective mitigation measure.

If you do decide to pay the ransom to avoid the data being published, you should still presume that the data is compromised and take actions accordingly. For example, the attacker may still decide to publish the data, share the data offline with other attack groups or further exploit it for their own gains. You still need to consider how you will mitigate the risks to individuals even though you have paid the ransom fee.

Scenario 8: Testing and assessing security controls

I want to protect my organisation and the personal data I process from ransomware. Is there any type of testing I can do to assess whether my controls are appropriate?

The UK GDPR requires you to regularly test, assess and evaluate the effectiveness of your technical and organisational controls using appropriate measures. There is no one test that you can carry out, you should consider this within your wider security framework.

For the examples discussed within this review, we have provided several suggested methods which will support you in adopting appropriate measures:

- **Breach notification**: Document and perform regular tests of your incident response plan so you are prepared for a real incident. The NCSC Exercise in a Box tool can help you practice your incident response in a safe environment.
- **Account management**: Regularly audit your user accounts to ensure they are still required and contain the appropriate privileges. This should include reviews to ensure staff have not retained privileges from previous internal job roles that are no longer required, often called "privilege creep". Ensure you document such reviews. Consider controls to identify weak or previously breached passwords.
- **Patch management**: Have a method to identify vulnerabilities in your network, such as missing patches. Vulnerability scans are an effective tool that can support this.
- **Attack tactics, techniques and procedure**: Risk assess and document your security controls to determine if they are appropriate to resist known TTPs. Penetration testers often simulate attacker activity by applying TTPs to vulnerabilities within your environment.
- **Audit**: Perform and record regular audits of your environment against a proven security standard, such as Cyber essentials (for smaller organisations) or ISO27001 (for medium and larger organisations).
- **Disaster recovery**: Perform and record regular tests of your disaster recovery plan to ensure it is effective. For example, perform a restore of personal data to ensure the data can be restored within the recovery time objective.

As with any tests, reviews, and assessments, ensure you document and appropriately retain these records, as you may need to submit them to the ICO.