Ransomware Recovery Plan for Small Businesses

Ransomware attacks are a cybersecurity threat to small and medium-sized businesses. These attacks can stop employees from accessing business files, applications, databases and essential IT systems. In some cases cybercriminals may also steal information and threaten to publish it unless a ransom is paid.

For UK businesses having a documented ransomware recovery procedure is essential for reducing downtime protecting important business information and restoring normal operations safely.

A ransomware recovery plan should be part of an IT Disaster Recovery Plan. It should explain who is responsible for responding to an incident, how affected systems will be isolated how backups will be protected and how business operations will be restored.

The following steps give a ransomware recovery framework that small businesses can adapt to their own IT environments.

Step 1: Identify and Isolate Affected Devices

The priority during a ransomware incident is to stop the attack from spreading to other computers, servers and network devices.

If an employee sees file encryption ransom messages or suspicious computer activity the employee should report the incident right away to the IT administrator or support provider.

Recommended actions include:

- Disconnect infected computers from wired and wireless networks.
- network connections to affected servers where necessary.
- Isolate compromised devices from shared folders and network storage.
- Prevent affected computers from accessing backup systems.
- Identify other devices showing unusual activity.
- Avoid connecting external backup drives to infected computers.

When possible isolation should be arranged by IT professionals so that systems that are still safe continue to run.

Step 2: Activate Your Incident Response Team

Once a ransomware incident has been identified the business should start its incident response procedure.

Every organisation should know who is responsible for managing the incident and making recovery decisions.

The incident response team may include:

- **Incident Coordinator:** Oversees the response and talks with management.
- **IT Administrator:** Looks at devices, user accounts and network systems.
- **External IT Support Provider:** Helps with containment, technical investigation and system recovery.

- **Management Representative:** Approves business decisions and recovery priorities.
- **Data Protection Lead:** Looks at exposure of personal and confidential information.

The incident coordinator should keep a record of events, decisions and actions taken throughout the recovery process.

Businesses should also keep a contact list that contains IT support details, software providers, backup providers and other external contacts.

Step 3: Protect and Assess Available Backups

Backups are one of the important parts of ransomware recovery.. Businesses should not assume that every backup is safe just because it was made before the incident.

Some ransomware attacks try to find and encrypt backup systems before demanding payment.

Businesses should:

- Find the recent available backup copies.
- Check whether backups are stored separately from the affected network.
- Confirm whether offline or immutable backups are available.
- Look at backup monitoring reports for activity.
- Find the clean backup before the attack.
- Verify that backup data can be restored successfully.
- Protect backup administrator accounts and access credentials.

The recovery team should check copies for integrity before using them to restore business systems.

A backup that has never been tested may not give the protection a business expects.

Step 4: Investigate the Incident and Assess the Damage

Before restoring systems businesses need to know how far the ransomware attack went.

The IT team should investigate how attackers got in which systems were affected and whether confidential information was accessed or stolen.

The investigation should look at:

- Which computers, servers and cloud services were affected?
- Were administrator or employee accounts compromised?
- Did the attack spread through shared network folders?
- Were business email accounts accessed?
- Was customer or employee information exposed?
- Were backups affected or deleted?
- Is there evidence of remote access?

Businesses should keep security logs, suspicious emails and other evidence. Do not delete affected files. Rebuild systems, before evidence has been collected.

If needed bring in a cybersecurity or incident response specialist.

Step 5: Rebuild and Secure Affected Systems

After identifying the systems and confirming the recovery approach the business can start rebuilding its IT environment.

I believe that restoring computers without fixing the underlying security problem can let attackers come back in.

1. Reinstall the operating systems with trusted installation media.
2. Apply the security updates and patches.
3. Remove any applications and suspicious configurations.
4. Reset passwords, for employees and administrators that have been compromised.
5. Enable -factor authentication (MFA).
6. Review administrator permissions and user access levels.
7. Check firewall, antivirus and endpoint security configurations.
8. Confirm that remote access services are properly secured.

Where possible I recommend that recovery should be carried out in an environment that has been checked for signs of compromise so that attackers cannot slip back in.

Step 6: Restore Business Data and Applications

Once the affected systems are secured the business can start restoring its applications and information.

Restoration should follow the recovery priorities that are written in the Disaster Recovery Plan.

For example a small business may prioritise:

1. Identity and administrator access.
2. Email and employee communication systems.
3. Essential business. Shared folders.
4. Accounting and invoicing applications.
5. Customer relationship management (CRM) systems.
6. Other. Non-essential services.

The recovery team should verify that restored files are accessible that applications work correctly and that business data is complete.

Where possible test restored systems before letting employees resume activities.

Step 7: Review the Incident and Improve Security

After recovering from a ransomware attack businesses should review what happened and identify improvements to prevent similar incidents.

The review should examine:

- How attackers initially gained access.
- Whether phishing emails or compromised passwords were involved.
- Whether existing security controls worked effectively.
- Whether backups were available. Could be restored.
- Whether the recovery process met the agreed RTO and RPO targets.
- Whether employees followed the incident reporting procedure.
- Which security improvements are required.

Businesses should update its Disaster Recovery Plan based on the lessons learned and communicate any changes to employees.

Ransomware Recovery Checklist for UK SMEs

Use this checklist as part of your business disaster recovery procedure.

Immediate Response

- Identify signs of ransomware infection.
- Report the incident to IT support and management.
- Disconnect affected devices from the network.
- Activate the incident response team.
- Record the time and details of the incident.

Investigation and Containment

- Identify affected computers, servers and accounts.
- Check for administrator activity.
- Investigate data exposure.
- Preserve security logs and evidence.
- Prevent access, to backup systems.

Recovery and Restoration

- Identify the verified clean backups.
- Rebuild affected systems securely.
- Reset compromised passwords.
- Enable multi-factor authentication.

- Restore business systems in priority order.
- Test restored. Business files.
- Confirm that employees can resume work.

Post-Incident Actions

- Assess UK GDPR reporting responsibilities.
- Document the incident and recovery actions.
- Review backup and security arrangements.
- Update the Disaster Recovery Plan.
- Provide employee cybersecurity training.

How Small Businesses Can Reduce the Risk of Future Ransomware Attacks

Recovering from ransomware can be expensive and disruptive. Small businesses should combine reliable backup arrangements with preventive cybersecurity measures.

Consider implementing the following controls:

- **Regular and Protected Backups:** Maintain regular backups of important business data and keep protected copies separate from everyday network access.
- **Multi-Factor Authentication:** Enable MFA for business email, administrator accounts, remote access and other important cloud services.
- **Employee Security Awareness:** Train employees to recognise phishing emails, suspicious attachments and unexpected login requests.
- **Software Updates:** Keep operating systems, business applications, firewalls and security software updated.
- **Access Control:** Give employees access only to the systems and information required for their roles.
- **Endpoint Protection:** Use appropriate antivirus and endpoint detection tools to identify and respond to suspicious activity.
- **Regular Recovery Testing:** Test backup restoration and disaster recovery procedures to confirm that the business can recover within its agreed recovery objectives.

A combination of preventive security controls, reliable backups and a documented recovery process can significantly improve an organisation's resilience against ransomware attacks.

How Computer Support Centre Can Help

Computer Support Centre helps UK small businesses improve their IT security, backup arrangements and disaster recovery readiness.

Our IT support services can help organisations review their existing backup arrangements, improve Microsoft 365 security, implement multi-factor authentication and establish practical IT recovery procedures.

Whether your business needs help preparing a Disaster Recovery Plan or reviewing its existing IT security arrangements, having the right support in place can make a significant difference when an unexpected incident occurs.