RANSOMWARE
RECOVERY CHECKLIST

MetaCompliance®

Ransomware Recovery Checklist

Ransomware is one of the most insidious and harmful forms of malware.

No matter what size your company is, ransomware causes damage.

A ransomware attack can paralyse operations, compromise sensitive data, and inflict severe financial and reputational damage.

Here are some ways to ensure your organisation does not suffer consequences of ransomware.

1) Isolate **Infected Machines:**

- Act swiftly to disconnect infected machines from the network.
- Disable Wi-Fi, Bluetooth, and any other networking capabilities.
- Unplug ethernet cables to prevent further spread.

2) Notify **IT Security Team:**

- Inform the IT security team immediately to contain and address the ransomware incident promptly.
- Ensure your IT team is well-versed in the organisation's incident response plan.

3) Report **the Incident:**

- Establish a clear incident reporting structure to facilitate timely identification and reporting by staff.
- Conduct regular training sessions to educate employees on recognising and reporting potential incidents.

4) Change **Login Credentials:**

- Promptly change all admin and user login credentials.
- Implement multi-factor authentication for an additional layer of security.

5) Document the Ransom Note:

- Capture a photo of the ransom note using a mobile device.
- Preserve the image as potential evidence.

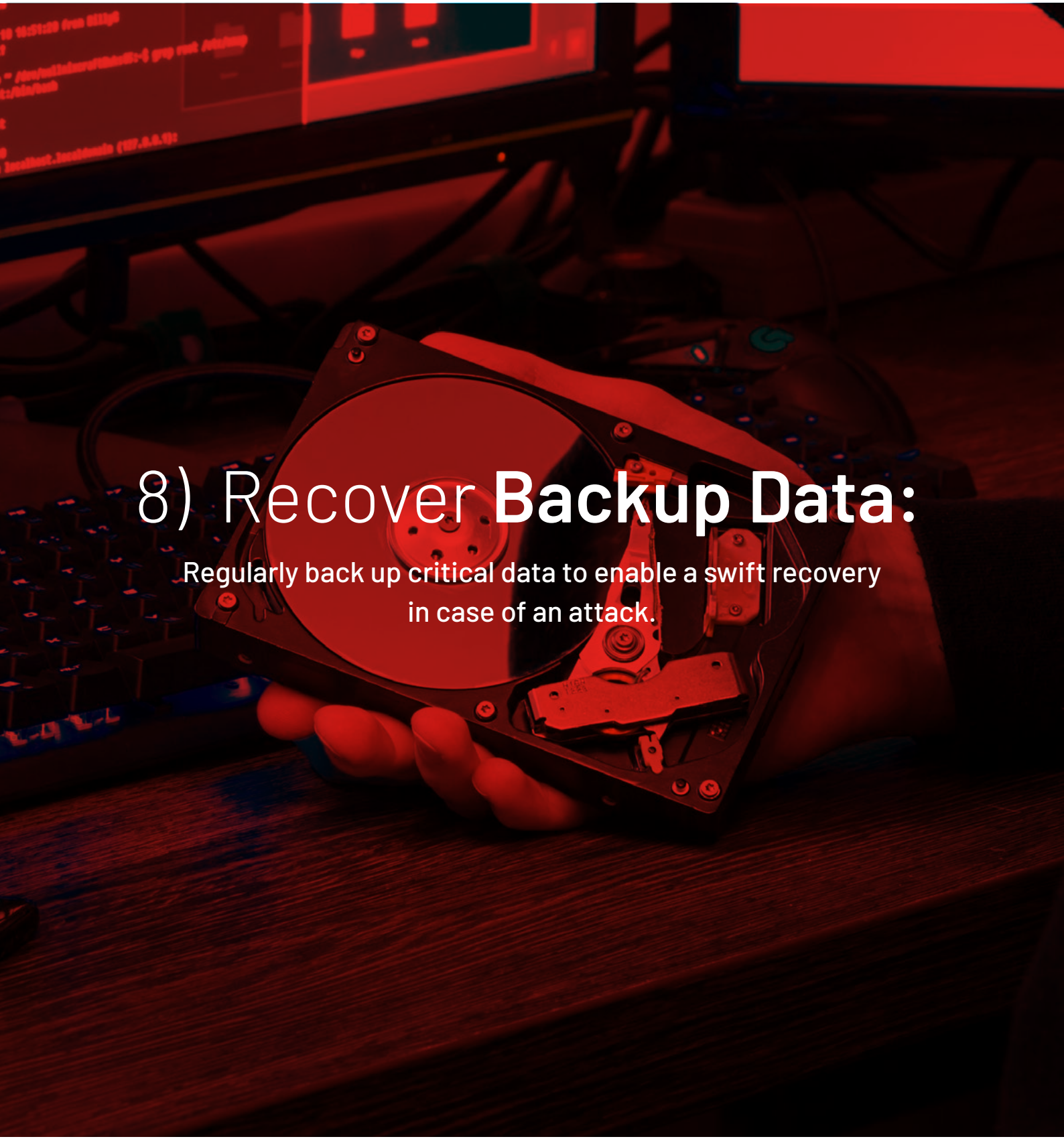
6) Do Not **Pay the Ransom:**

- Understand that paying the ransom is not a guarantee of file recovery.
- Avoid making payments, as it encourages cybercriminals and may lead to repeated attacks.

7) Update Systems:

- Conduct a thorough security audit post-incident to identify vulnerabilities.
- Ensure that all systems, software, and applications are promptly updated to the latest versions to patch potential security holes.

MetaCompliance®



8) Recover **Backup Data:**

Regularly back up critical data to enable a swift recovery in case of an attack.

RANSOMWARE
RECOVERY CHECKLIST:

1) Isolate **Infected Machines** ❑
2) Notify **IT Security Team** ❑
3) Report **the Incident** ❑
4) Change **Login Credentials** ❑
5) Document **the Ransom Note** ❑
6) Do Not **Pay the Ransom** ❑
7) Update **Systems** ❑
8) Recover **Backup Data** ❑

MetaCompliance®