Ransomware Readiness Checklist by Callnet Solution

Think your business is ready to face ransomware? This quick checklist will help you find out. If you're unsure about any point, talk to our cybersecurity experts for deeper guidance and remediation steps.

1. Prevention

- ☐ All email accounts are protected by advanced filtering to block phishing, malicious attachments, and spoofed senders.
- ☐ Endpoint protection or EDR is installed, updated, and centrally managed.
- ☐ Operating systems, apps, and plugins are patched within days of security updates.
- ☐ Multi-factor authentication (MFA) is enforced for VPN, admin logins, and critical systems.

2. Detection

- ☐ Systems are monitored for unusual file changes, mass encryption activity, or abnormal login attempts.
- ☐ Alerts are configured to trigger immediately when suspicious behaviour is detected.
- ☐ Canary files or honeypots are deployed as early-warning traps.

3. Containment & Response

- ☐ Staff know how to isolate an infected device (disconnect network and Wi-Fi) within minutes.
- ☐ Your network is segmented so an infection cannot spread freely.
- ☐ A documented incident response plan exists — and the team has rehearsed it in the past 12 months.

4. Recovery

- ☐ Backups follow the 3-2-1 rule (three copies, two types of storage, one offsite).
- ☐ Backups are immutable and encrypted both in transit and at rest.
- ☐ Restore drills confirm RPO (data loss tolerance) and RTO (recovery speed) targets can be met.

If you can't confidently check every box, your business may be at risk.

Contact Callnet Solution for a free ransomware consultation and get expert, local guidance on strengthening your defences before it's too late.