Ransomware Readiness Checklist

A quick-assessment tool to evaluate how well your business can prevent, detect, and recover from ransomware.

1. Prevention Measures

1. [ ] Multi-factor authentication (MFA) is enabled for all remote access points
2. [ ] All software and operating systems are kept up to date with automatic patching enabled
3. [ ] RDP, VPN, and other remote services are protected and not exposed to the public internet
4. [ ] Employees receive ongoing training to detect phishing and social engineering attempts

2. Detection Capabilities

1. [ ] EDR or MDR is deployed with behavioral detection, not just signature-based antivirus
2. [ ] Security logs are collected and reviewed regularly (or monitored by a service)
3. [ ] Alerts are configured for unusual activity like privilege escalation or mass file changes
4. [ ] Can isolate a device from the network if compromise is suspected

3. Response Planning

1. [ ] You have an incident response plan, and it includes ransomware-specific procedures
2. [ ] At least one team member knows how to shut down and contain a threat quickly
3. [ ] Legal, compliance, and public relations considerations are part of your plan
4. [ ] You have a trusted IT/security provider to call in the event of an attack

4. Recovery Assurance

1. [ ] Backups are automated, encrypted, and tested monthly
2. [ ] At least one backup is offline, air-gapped, or stored immutably
3. [ ] You can restore key systems from backup in under 24 hours
4. [ ] You have documented and tested your recovery process

Want expert help evaluating your ransomware defenses?
Contact Wentz IT Consulting for a comprehensive security posture review.
https://wentzitconsulting.com/contact