Q3 Cybersecurity Readiness Checklist

Mid-Year Risk Management for Small Businesses

Ensure your business is secure, compliant, and prepared for Q3 and beyond with this essential cybersecurity checklist from GeorgiaMSP.

✅ Core Security Infrastructure

- ☐ All operating systems and software are fully updated
- ☐ Firewalls are configured and functioning properly
- ☐ Antivirus and anti-malware tools are current and actively monitored
- ☐ All company devices (laptops, mobile, IoT) are enrolled in endpoint protection
- ☐ Remote access solutions (VPN, RDP, etc.) are secured with MFA

✅ Data Protection & Backup

- ☐ Automated daily backups are running successfully
- ☐ Backups are encrypted and stored offsite or in the cloud
- ☐ Backup restoration process was tested in the last 60 days
- ☐ Sensitive data is encrypted at rest and in transit
- ☐ Data retention policies are clearly defined and enforced

✅ Access Control & Identity Management

- ☐ MFA (Multi-Factor Authentication) is enabled on all critical systems
- ☐ Inactive user accounts have been reviewed and removed
- ☐ Role-based access control (RBAC) is in place
- ☐ Password policy requires strong, unique passwords

- ☐ Privileged accounts are audited monthly

✅ Employee Awareness & Training

- ☐ All staff completed cybersecurity awareness training this year
- ☐ Phishing simulation was conducted in Q2 or scheduled for Q3
- ☐ Staff understands how to report suspicious emails or activities
- ☐ Policy reminders (acceptable use, remote work, BYOD) were distributed
- ☐ Social engineering awareness training has been refreshed

✅ Monitoring & Threat Detection

- ☐ Security Information & Event Management (SIEM) system is in place
- ☐ Threat alerts and logs are actively monitored
- ☐ Suspicious activity is investigated within 24 hours
- ☐ Incident Response Plan has been reviewed and updated
- ☐ Endpoint Detection & Response (EDR) tools are deployed

✅ Compliance & Documentation

- ☐ Cybersecurity policies were reviewed in the last 6 months
- ☐ Regulatory compliance requirements (e.g., HIPAA, PCI-DSS) are being met
- ☐ Cyber insurance policy is active and adequate for current risk level
- ☐ Business continuity and disaster recovery plans are current
- ☐ Third-party/vendor cybersecurity policies are reviewed annually

---

✅ Q3 Priorities

- ☐ Schedule an external vulnerability scan or penetration test
- ☐ Perform a security risk assessment

- ☐ Update inventory of all connected devices and software
- ☐ Host a cybersecurity refresher lunch-and-learn for employees
- ☐ Schedule a Q3 review call with GeorgiaMSP

Need Help With Any of These?

GeorgiaMSP can assist with every item on this checklist. Whether it’s a one-time assessment or fully managed cybersecurity, we’re here to protect your business.

📞 **Call:** +1 404-418-5300
📧 **Email:** info@georgiamsp.com
🌐 **Visit:** www.georgiamsp.com