Micro Strategies
microstrat.com

Your score
__/13

Cybersecurity Controls Self-Assessment

Check off each control your organization has fully in place. "Fully in place" means actively managed — not just purchased or partially deployed. Use your score to start a conversation with your IT team or security partner.

IDENTIFY & ACCESS

- ☐ **Multi-factor authentication (MFA)**
  Enabled across email, remote access, and critical business systems — not just one
- ☐ **Strong password policies**
  Enforced complexity and rotation; no shared or default credentials in use
- ☐ **Administrative account separation**
  Admin accounts used only for admin tasks, not everyday work

EMAIL & COMMUNICATIONS

- ☐ **Email security protections**
  Filtering, anti-phishing, and attachment scanning actively in place
- ☐ **SPF, DMARC, and DKIM configured**
  Protects your domain from being spoofed in phishing attacks targeting your clients

PEOPLE & POLICY

- ☐ **Security awareness training**
  Regular training and phishing simulations for all staff, not just onboarding
- ☐ **Cybersecurity insurance**
  Active policy with coverage reviewed annually against current controls

ENDPOINT & INFRASTRUCTURE

- ☐ **Endpoint detection & response (EDR)**
  Active monitoring on all endpoints — not just traditional antivirus
- ☐ **Patch & vulnerability management**
  Regular patching cadence for OS, applications, and firmware across all devices
- ☐ **Firewall management**
  Actively managed with current rules — not default settings from original installation
- ☐ **Intrusion detection / prevention**
  Network-level monitoring for suspicious activity, not just perimeter blocking

RESILIENCE & RECOVERY

- ☐ **Off-site and immutable backups**
  Backups stored separately and protected from ransomware encryption; tested regularly
- ☐ **Logging and monitoring**
  Activity logs retained and actively reviewed — not just stored and ignored

HOW TO INTERPRET YOUR SCORE

0-4	5-8	9-11	12-13
At risk	**Partial coverage**	**Strong foundation**	**Well protected**
Significant exposure. Priority action needed before an incident occurs.	Some controls in place, but gaps remain that attackers actively exploit.	Well positioned. Focus on closing remaining gaps and keeping controls current.	Comprehensive posture. Maintain active management — threats evolve constantly.

Not sure how to answer some of these? That's the conversation worth having.