Cybersecurity Self-Assessment

20 questions. Five essential areas. One clear starting point.

Assess what your organization has in place today across Identify, Protect, Detect, Respond, and Recover. This quick self-check helps highlight areas to discuss and improve.

HOW TO SCORE

For each statement, select Yes (1 point) if the safeguard is consistently in place today, or No / Unsure (0 points) if it is missing, inconsistent, or you cannot confirm it. Do not award points for planned improvements.

Each area: 0-4 points | Overall: 0-20 points | Estimated time: 5-10 minutes

01 IDENTIFY / 4 POINTS

SECURITY READINESS STATEMENT	YES 1	NO / UNSURE 0
We maintain an up-to-date inventory of business devices, software, and critical systems.	[ ]	[ ]
We know which business data and systems are most important to protect.	[ ]	[ ]
Someone is clearly responsible for cybersecurity decisions and oversight.	[ ]	[ ]
We periodically review cybersecurity risks, including vendor and third-party risks.	[ ]	[ ]

Identify score: _____ / 4

02 PROTECT / 4 POINTS

SECURITY READINESS STATEMENT	YES 1	NO / UNSURE 0
Multi-factor authentication (MFA) protects email, remote access, and other critical accounts.	[ ]	[ ]

SECURITY READINESS STATEMENT	YES 1	NO / UNSURE 0
Access is limited to what employees need and removed promptly when they leave.	[ ]	[ ]
Devices and software receive timely security updates and are protected against malware.	[ ]	[ ]
Employees receive cybersecurity awareness training, including phishing guidance.	[ ]	[ ]

Protect score: _____ / 4

03 DETECT / 4 POINTS

SECURITY READINESS STATEMENT	YES 1	NO / UNSURE 0
Security alerts and important system activity are monitored for suspicious behavior.	[ ]	[ ]
We have a process to identify and report suspected phishing, unusual logins, or malware.	[ ]	[ ]
Security logs and alerts are reviewed by a responsible person or service.	[ ]	[ ]
We can recognize and investigate signs that a security control has failed.	[ ]	[ ]

Detect score: _____ / 4

04 RESPOND / 4 POINTS

SECURITY READINESS STATEMENT	YES 1	NO / UNSURE 0
We have a documented plan for handling a cybersecurity incident.	[ ]	[ ]
Employees know whom to contact immediately when they suspect an incident.	[ ]	[ ]
We can quickly isolate affected devices or accounts to limit damage.	[ ]	[ ]
We review or practice our incident response process at least annually.	[ ]	[ ]

Respond score: _____ / 4

05 RECOVER / 4 POINTS

SECURITY READINESS STATEMENT	YES 1	NO / UNSURE 0
Critical business data is backed up on a defined schedule.	[ ]	[ ]
At least one protected backup copy is isolated from everyday user access or is immutable.	[ ]	[ ]
We periodically test restoring data from backups.	[ ]	[ ]
We have documented recovery priorities and a plan to resume critical operations.	[ ]	[ ]

Recover score: _____ / 4

Your Cybersecurity Readiness Score

Count each Yes as 1 point. Each No / Unsure is 0 points. Add the five section scores for your total.

YOUR RESULTS

Identify	_____ / 4
Protect	_____ / 4
Detect	_____ / 4
Respond	_____ / 4
Recover	_____ / 4
OVERALL TOTAL	**_____ / 20**

WHAT YOUR SCORE SUGGESTS

0-9 | Needs attention - Several foundational safeguards may be absent or unverified.

10-15 | Developing - Some safeguards are in place, but meaningful gaps may remain.

16-20 | Stronger foundation - Many foundational safeguards are reported as in place. Continue verifying and testing them.

Your lowest-scoring area: _____

NEXT STEPS

Prioritize any No / Unsure answers, especially those involving MFA, security updates, monitoring, incident response, and recoverable backups. A high score does not guarantee protection against cyberattacks.

CONTACT CSG TECHNOLOGIES
Review your results, discuss your IT environment, and identify practical next steps.
(904) 296-4811 | support@csgtechnologies.net
csgtechnologies.net/contact-us/