FREE BUSINESS WORKBOOK

The 15-Minute Small Business Ransomware Readiness Check

Find out whether your business could contain a ransomware attack before it spreads - no cybersecurity experience required.

12	PRACTICAL QUESTIONS
15	MINUTES TO COMPLETE
03	PRIORITIES TO TAKE FORWARD

TALLGRASS SIGNAL
Security operations + AI solutions engineering

HOW TO USE THIS CHECK

Answer what is true today - not what the policy says should be true.

For each statement, choose Yes, Partly / Not sure, or No. If you do not know, choose Partly / Not sure. Uncertainty is itself useful: it identifies where evidence or ownership is missing.

YES	1 point	The control exists, is consistently applied, and can be demonstrated.
PARTLY / NOT SURE	1/2 point	Coverage is incomplete, informal, untested, or you cannot verify it.
NO	0 points	The control is not currently in place.

YOUR SCORE

0-4	**HIGH EXPOSURE**	Start with identity, endpoint visibility, and recoverable backups.
5-7	**SIGNIFICANT GAPS**	Several gaps could allow an attack to spread or delay recovery.
8-10	**GOOD FOUNDATION**	Useful controls exist; now close gaps and test them together.
11-12	**WELL PROTECTED**	Validate the system under pressure and maintain evidence.

This is a directional planning tool, not a technical audit, certification, insurance opinion, or guarantee that an attack will be prevented.

IDENTITY

Control the keys to the business.

Mark one answer for each question. If proof is unavailable, choose Partly / Not sure.

01 / IDENTITY

Is multifactor authentication required for email, remote access, and administrator accounts?

Strong coverage includes every privileged and externally accessible account, not just some employees.

[ ] YES +1	[ ] PARTLY / NOT SURE +1/2	[ ] NO +0

02 / IDENTITY

Do administrators use separate accounts for privileged work instead of daily email and browsing?

Separate administrative access limits what an attacker can do with one compromised account.

[ ] YES +1	[ ] PARTLY / NOT SURE +1/2	[ ] NO +0

03 / IDENTITY

Are former employees and contractors removed promptly from email, cloud applications, and remote access?

A repeatable offboarding process prevents forgotten accounts from becoming an easy way back in.

[ ] YES +1	[ ] PARTLY / NOT SURE +1/2	[ ] NO +0

ENDPOINTS

See and contain what is happening on company devices.

Mark one answer for each question. If proof is unavailable, choose Partly / Not sure.

04 / ENDPOINTS

Can your team confirm that every active laptop, workstation, and server has current, centrally managed endpoint protection?

A reliable inventory includes remote devices and systems that rarely connect to the office network.

[ ] YES +1	[ ] PARTLY / NOT SURE +1/2	[ ] NO +0

05 / ENDPOINTS

Can your IT or security team isolate a suspicious device quickly without being physically present?

Fast remote isolation can stop one compromised endpoint from reaching shared systems.

[ ] YES +1	[ ] PARTLY / NOT SURE +1/2	[ ] NO +0

BACKUPS

Make recovery possible after production systems are affected.

Mark one answer for each question. If proof is unavailable, choose Partly / Not sure.

06 / BACKUPS

Are critical backups protected from the same accounts and systems used in daily operations?

Attackers often target accessible backups before encrypting production data.

[ ] YES +1	[ ] PARTLY / NOT SURE +1/2	[ ] NO +0

07 / BACKUPS

Has your team successfully restored important data or a critical system within the last six months?

A completed restore test is stronger evidence than a backup dashboard showing green status.

[ ] YES +1	[ ] PARTLY / NOT SURE +1/2	[ ] NO +0

RESPONSE

Know who acts, who decides, and how they communicate.

Mark one answer for each question. If proof is unavailable, choose Partly / Not sure.

08 / RESPONSE

Is one person clearly authorized to coordinate technical and business decisions during a cyber incident?

A named owner reduces delay when IT, leadership, insurance, legal counsel, and communications must align.

[ ] YES +1	[ ] PARTLY / NOT SURE +1/2	[ ] NO +0

09 / RESPONSE

Can your team reach critical response contacts without relying on company email?

Ransomware can make normal email, files, and contact lists unavailable when they are needed.

[ ] YES +1	[ ] PARTLY / NOT SURE +1/2	[ ] NO +0

RECOVERY + INSURANCE

Restore the business in the right order - and know what you represented.

Mark one answer for each question. If proof is unavailable, choose Partly / Not sure.

10 / RECOVERY

Has leadership identified which business systems and processes must return first?

Recovery is faster when technical restoration follows agreed business priorities.

[ ] YES +1	[ ] PARTLY / NOT SURE +1/2	[ ] NO +0

11 / RECOVERY

Has the organization practiced a ransomware or major-outage scenario in the last year?

A short tabletop exercise exposes unclear authority, missing contacts, and unrealistic assumptions.

[ ] YES +1	[ ] PARTLY / NOT SURE +1/2	[ ] NO +0

12 / INSURANCE

Do you know whether your cyber-insurance policy requires EDR, multifactor authentication, or continuous monitoring?

Confirm policy requirements and representations with your broker or insurer. This checklist is not legal or insurance advice.

[ ] YES +1	[ ] PARTLY / NOT SURE +1/2	[ ] NO +0

SCORE + PRIORITIZE

Turn the answers into the next three moves.

Add 1 point for each Yes and 1/2 point for each Partly / Not sure. Then circle the three incomplete controls that would most affect your ability to contain an attack or restore operations.

QUESTION	SCORE	OWNER / EVIDENCE
01. Is multifactor authentication required for email, remote access, and administrator accounts?	____	_____
02. Do administrators use separate accounts for privileged work instead of daily email and browsing?	____	_____
03. Are former employees and contractors removed promptly from email, cloud applications, and remote access?	____	_____
04. Can your team confirm that every active laptop, workstation, and server has current, centrally managed endpoint protection?	____	_____
05. Can your IT or security team isolate a suspicious device quickly without being physically present?	____	_____
06. Are critical backups protected from the same accounts and systems used in daily operations?	____	_____
07. Has your team successfully restored important data or a critical system within the last six months?	____	_____
08. Is one person clearly authorized to coordinate technical and business decisions during a cyber incident?	____	_____
09. Can your team reach critical response contacts without relying on company email?	____	_____
10. Has leadership identified which business systems and processes must return first?	____	_____
11. Has the organization practiced a ransomware or major-outage scenario in the last year?	____	_____
12. Do you know whether your cyber-insurance policy requires EDR, multifactor authentication, or continuous monitoring?	____	_____
TOTAL	**____ / 12**	

THE GAP THAT MATTERS

Having security software is not the same as having security monitoring.

Traditional antivirus can block known malicious files. Modern endpoint detection and response (EDR) adds behavioral detection, richer investigation context, and response actions such as remote isolation. The operating model matters just as much: someone must maintain coverage, review meaningful alerts, coordinate action, and explain what happened.

TRADITIONAL ANTIVIRUS	MANAGED ENDPOINT SECURITY
Primarily looks for known malicious files and patterns.	Adds behavioral visibility, investigation context, and managed operational ownership.
May alert on a device without giving the business a response process.	Creates a defined path for triage, containment decisions, coordination, and reporting.
Coverage gaps may be difficult to see across remote and infrequently connected devices.	Reconciles agent health and device coverage so missing protection becomes visible.
An alert is still only an alert.	The value is the operating layer around the technology - accountability, evidence, and action.

ASK YOUR IT PROVIDER

+ Can you show me which company devices are currently protected?
+ Who reviews alerts, during what hours, and how quickly?
+ Can you isolate a remote device without touching it?
+ When was our last successful restore test?
+ What happens first if ransomware is suspected?

YOUR NEXT MOVE

Do not fix twelve things at once.

Choose three actions with clear owners and evidence. If endpoint visibility, isolation, or alert handling is unclear, that is a natural place to evaluate managed endpoint security.

COMPLIMENTARY 20-MINUTE REVIEW

Not sure what your answers mean?

Tallgrass Signal will review your result and identify the three highest-priority gaps - without turning the conversation into a technical lecture.

EMAIL hello@tallgrasssignal.com
WEB tallgrasssignal.com/ransomware-readiness

ABOUT TALLGRASS SIGNAL

Tallgrass Signal is a focused security operations and AI solutions engineering practice serving growing organizations across Eastern Iowa. We help businesses turn endpoint telemetry into clear investigation, coordinated action, and ongoing risk reduction.

This workbook is educational. It does not provide legal, insurance, compliance, or incident-response advice and does not guarantee prevention, detection, containment, or recovery.