

Cybersecurity Readiness: Could Your Business Respond?

Instructions: Select a business-critical operation and consider what would happen if a cyber incident disrupted its supporting systems.

	READINESS AREA	QUESTION TO ANSWER	WARNING SIGNS	CONFIRMED	NEEDS VALIDATION	GAP IDENTIFIED
	Critical Operations	Which business functions and systems must remain available or be restored first?	Unknown dependencies, undefined recovery priorities	☐	☐	☐
	Vulnerability Management	Are the most consequential exposures identified, prioritized, and assigned?	Unowned findings, overdue remediation, unverified fixes	☐	☐	☐
	Incident Detection	How would the organization recognize and escalate a potential compromise?	Unclear monitoring coverage, inconsistent escalation	☐	☐	☐
	Incident Response	Who makes containment and recovery decisions?	Outdated plans, undefined authority, untested procedures	☐	☐	☐
	Business Continuity	Can essential operations continue during an outage?	No alternative workflows, undocumented dependencies	☐	☐	☐
	Recovery	Have critical systems and data been successfully restored in a test?	Untested backups, unclear recovery objectives	☐	☐	☐

What did the review reveal?

- ☐ A critical process has undocumented dependencies.
 ☐ A response procedure needs to be tested.
- ☐ A vulnerability requires additional investigation or remediation.
 ☐ Backup or recovery capabilities need validation.
- ☐ Incident response ownership needs clarification.
 ☐ A continuity gap requires leadership attention.

Priority readiness gap: _____

Potential business impact: _____

Responsible owner: _____

Next action and due date: _____



Remember: Readiness is not demonstrated by the existence of a plan. It is demonstrated by the organization's ability to execute that plan when needed.