DATAPRISE

CYBERSECURITY READINESS SCORECARD

How prepared is your organization for today's threats



A cyber incident doesn't become costly because it happens. It becomes costly because organizations aren't prepared to detect, respond, and recover quickly.

This assessment will help you evaluate your organization's cybersecurity readiness across five critical areas and identify potential gaps before they become business risks.

Ask yourself:

"How quickly would we know if we've been breached?"



01 Visibility & Monitoring

Know what's happening across your environment.

02 Threat Detection & Response

Identify and contain threats quickly.

03 Vulnerability Management

Find and remediate security weaknesses.

04 Recovery & Resilience

Ensure business continuity after an incident.

05 Security Governance

Align cybersecurity with business risk.

01

Visibility & Monitoring

- ❑ We have 24x7 monitoring of critical systems, endpoints, and cloud environments.
- ❑ We can quickly identify suspicious activity across our network from a centralized dashboard.
- ❑ We have visibility into both on-premises and cloudbased assets.

02

Threat Detection & Response

- ❑ We can detect and investigate potential threats within minutes, not days.
- ❑ We have a documented incident response plan that has been tested within the last 12 months.
- ❑ Key stakeholders know their roles and responsibilities during a cybersecurity incident.

03

Vulnerability Management

- ❑ Critical vulnerabilities are identified, prioritized, and remediated through a structured process.
- ❑ We conduct regular vulnerability assessments and penetration testing.
- ❑ Security findings are prioritized based on business risk, not just technical severity.

04

Recovery & Resilience

- ❑ We maintain secure, tested backups of critical business systems.
- ❑ At least one backup or recovery path is immutable and protected from ransomware attacks.
- ❑ We have tested our ability to recover critical systems within acceptable business timelines.

05

Security Governance

- ❑ We regularly review cybersecurity risks with executive leadership.
- ❑ We have defined security policies that are reveiwed and updated annually.
- ❑ Our security startegy is aligned with broader business objectives and compliance requirements.

Scoring

1 point per "**Yes**" answer.
Total possible points: 15.

13-15 YES
Strong Foundation

8-12 YES
Moderate Maturity

0-7 YES
Elevated Risk

Don't know the answer? *Count it as a "No."*

One of the most common risks we see is uncertainty around cybersecurity ownership, monitoring, and esponse readiness.



Want a Second Opinion?

Dataprise offers a complimentary cybersecurity assessment designed to help organizations identify gaps, benchmark their security posture, and receive practical recommendations for improvement.

Schedule Your FREE Cybersecurity Assessment