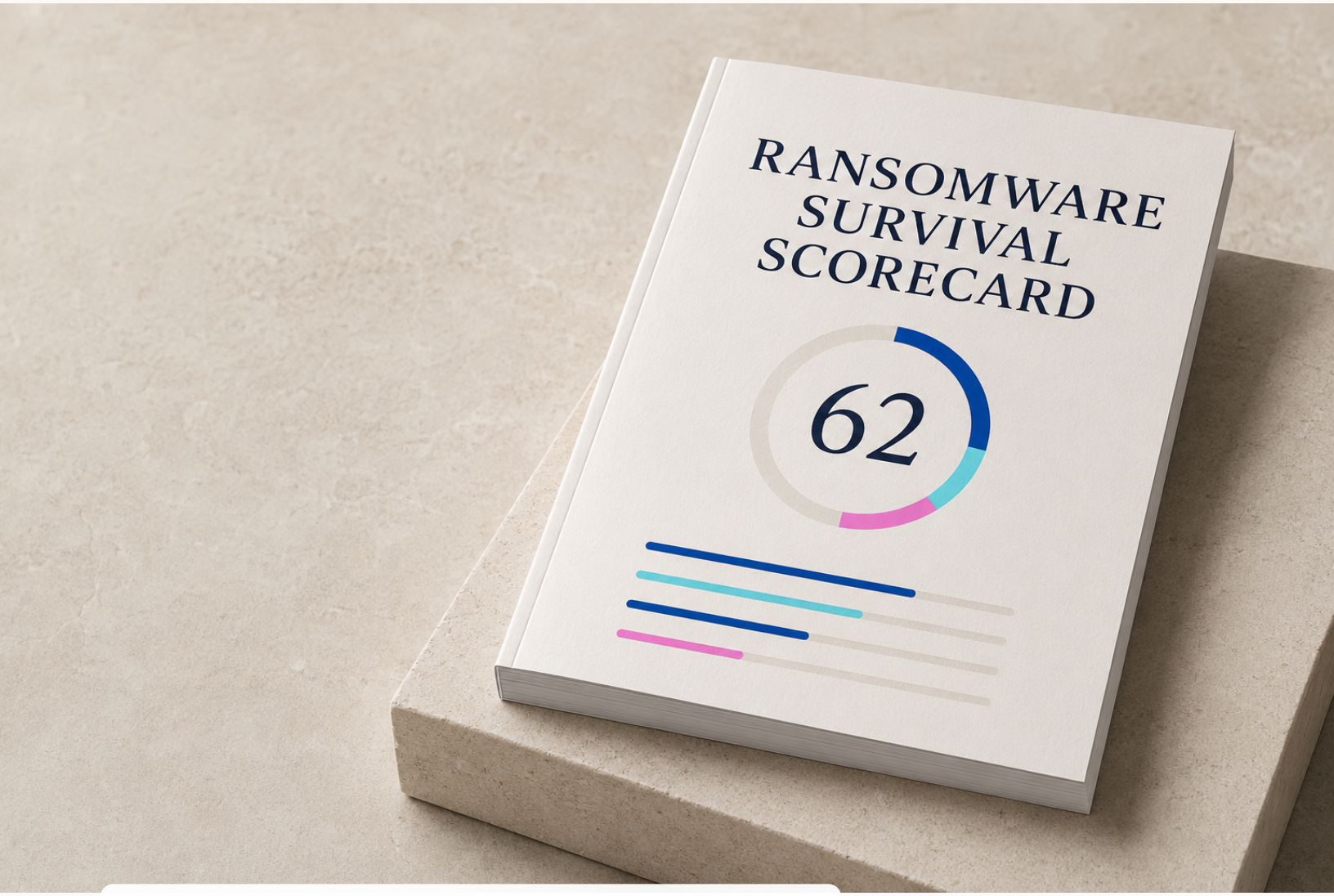
ATOMIC GUARDIAN

EXECUTIVE BRIEFING AND MANAGEMENT SCORECARD

Would your business survive ransomware?

A practical management guide to the controls, recovery evidence, and decisions that determine whether an attack becomes a disruption or a business crisis.



MORE INFORMATION

Use this briefing to prepare for a Ransomware Survival Assessment.

The question most businesses cannot answer with evidence

Security software can reduce the likelihood of compromise. Backups can preserve data. Neither proves that critical operations can be restored quickly, cleanly, and in the right order after a real ransomware event.

1

PREVENTION

Are identities, endpoints, email, remote access, and vulnerabilities actively hardened and monitored?

2

CONTAINMENT

Can compromised accounts and devices be isolated before the attack spreads across the business?

3

RECOVERY PROOF

Can management show what will be restored, from which clean copy, in what order, and approximately how long it will take?

The real test of cybersecurity is not whether you are attacked.

It is whether your business survives.

Seven questions management should be able to answer

1. Which systems must be restored within 4, 8, and 24 hours?
2. Is at least one critical backup inaccessible using normal production credentials?
3. Has a complete system or application restore been tested in the past 90 days?
4. Can compromised accounts and devices be isolated rapidly?
5. Are Microsoft 365, Google Workspace, and critical SaaS platforms independently backed up?
6. Does management have a written incident decision and communications plan?
7. Can essential operations continue while systems are being rebuilt?

IMPORTANT
These questions are an initial management screen. They do not replace a technical assessment, restore test, or incident exercise.

Prevent. Detect. Contain. Recover. Prove it.

PREVENT

Reduce the probability of compromise

Identity hardening, MFA, privileged access, patching, endpoint protection, email security, remote-access control, and employee readiness.

DETECT

Find malicious activity early

Managed monitoring, endpoint telemetry, identity signals, email visibility, network events, and defined escalation paths.

CONTAIN

Limit the blast radius

Rapid account disablement, endpoint isolation, segmentation, controlled administration, protected logs, and out-of-band communications.

RECOVER

Preserve a recoverable business

Isolated recovery copies, separate backup administration, cloud and SaaS protection, clean recovery environments, and defined recovery objectives.

PROVE IT

Test that recovery works

File and application restores, complete-system tests, measured recovery times, tabletop exercises, documented failures, and management evidence.

What the Ransomware Survival Assessment examines

01
Critical operations and downtime tolerance

02
Identity and administrative access

03
Endpoint and server controls

04
Email and cloud platforms

05
Network segmentation and remote access

06
Backup coverage and isolation

07
Restore-test history

08
Incident-response readiness

09
Business-continuity procedures

10
Cyber-insurance requirements

11
Third-party and vendor exposure

12
Production and operational dependencies

THE OBJECTIVE

Determine whether the business can restore critical operations, identify the most important recovery gaps, and establish a practical remediation sequence.

What management receives

1. **Executive resilience rating**
2. **Immediate critical findings**
3. **Estimated recovery gaps**
4. **Prioritized 30-, 60-, and 90-day remediation plan**
5. **Plain-language management report**
6. **Recommended resilience architecture**
7. **Budgetary implementation estimate**

THE COMMERCIAL PATH

Assessment -> Resilience build -> Managed proof

The assessment is a fixed-scope professional engagement. It turns uncertainty into an evidence-based remediation plan. When appropriate, Atomic Guardian can then implement the improvements and maintain the controls through an ongoing managed program.

ATOMIC GUARDIAN

YOUR INITIAL MANAGEMENT SCREEN

Count how many answers you can confirm with evidence.

6-7 CONFIRMED

Recovery ready

You may have a strong foundation. The assessment validates that the evidence and technical controls support management's view.

3-5 CONFIRMED

Material recovery gaps

Important controls or recovery evidence are uncertain. A structured assessment should identify the highest-priority gaps.

0-2 CONFIRMED

High risk of extended disruption

The business may be relying on assumptions rather than verified recovery capability. Prompt assessment is warranted.

Do not guess. Prove your business can recover.

BOOK A RANSOMWARE SURVIVAL ASSESSMENT

https://atomicguardian.com/book-a-call/

Secure, dependable IT for businesses that cannot afford disruption.