

SEVENCORE IT STRATEGY GROUP

Executive Brief

HOW HEALTHY IS YOUR IT ENVIRONMENT?

10 Warning Signs Your Technology Needs Executive Attention

The Executive IT Health Scorecard

Technology problems rarely begin with a major outage.

They usually start quietly.

An aging server that hasn't been replaced. A critical system only one employee understands. A vendor contract that hasn't been reviewed in years. Backups everyone assumes are working. Technology purchases made outside IT. Infrastructure decisions made without a long-term strategy.

Individually, these issues may appear manageable. Collectively, they can create significant **financial, operational, cybersecurity, and business continuity risk**.

For executive leadership, the question isn't simply:

"Is our technology working?"

The better question is:

"Is our technology environment resilient, secure, cost-effective, and capable of supporting where the business is going?"

Use this SevenCore Executive IT Health Scorecard to identify areas that may require leadership attention.

THE EXECUTIVE IT HEALTH SCORECARD

For each statement, select the answer that most accurately describes your organization.

YES — We have confidence in this area.

UNSURE — We cannot confidently verify it.

NO — This represents a known concern.

1. Aging Infrastructure

SEVENCORE IT STRATEGY GROUP

Executive Brief

Can leadership clearly identify which critical technology assets are approaching end-of-life or require replacement within the next 12–36 months?

Aging infrastructure doesn't necessarily mean failing infrastructure. The greater risk is operating critical systems without understanding their lifecycle, replacement costs, dependencies, or business impact.

Warning signs include:

- Aging servers, network equipment, storage, or communications systems
- Increasing maintenance requirements
- Hardware beyond recommended lifecycle
- Technology replacement driven by emergencies rather than planning
- No multi-year infrastructure lifecycle strategy

Executive concern: Unexpected capital expenses, downtime, performance degradation, and increased operational risk.

Your Score: YES / UNSURE / NO

2. Single Points of Failure

If one critical system, connection, vendor, device, or employee became unavailable tomorrow, could the business continue operating?

Technology resilience depends on understanding where the organization has concentrated risk.

Single points of failure may exist within:

- Internet connectivity
- Network infrastructure
- Servers and applications
- Telecommunications
- Cloud services
- Power
- Key technology personnel
- Vendors and service providers

Executive concern: One failure could interrupt an entire business process or operation.

Your Score: YES / UNSURE / NO

SEVENCORE IT STRATEGY GROUP

Executive Brief

3. Unsupported or Legacy Systems

Does leadership know whether any critical business systems are unsupported, obsolete, or approaching end-of-support?

Legacy technology can remain operational for years, creating the perception that replacement isn't necessary.

The problem emerges when the organization needs security updates, vendor support, replacement parts, integration, or emergency recovery.

Executive concern: Increased cybersecurity exposure, compatibility problems, higher support costs, and difficult recovery during an outage.

Your Score: YES / UNSURE / NO

4. Documentation Gaps

Could another qualified technology professional understand and support your environment without relying heavily on institutional knowledge?

Critical infrastructure should not exist primarily inside someone's head.

Organizations should maintain current documentation covering areas such as:

- Network architecture
- Technology assets
- System configurations
- Vendor relationships
- Administrative responsibilities
- Recovery procedures
- Critical dependencies

Executive concern: Knowledge concentration creates operational dependency and makes transitions, outages, audits, and recovery significantly more difficult.

Your Score: YES / UNSURE / NO

SEVENCORE IT STRATEGY GROUP

Executive Brief

5. Shadow IT

Does your organization have visibility into the technology, cloud applications, AI tools, subscriptions, and software employees are purchasing or using outside approved processes?

Technology purchasing is increasingly decentralized.

Departments can deploy applications with a credit card in minutes—sometimes without IT, cybersecurity, procurement, or executive leadership knowing they exist.

Shadow IT can introduce:

- Duplicate technology spending
- Uncontrolled data exposure
- Cybersecurity vulnerabilities
- Compliance concerns
- Integration problems
- Vendor sprawl

Executive concern: The organization cannot effectively manage technology risk or spending it cannot see.

Your Score: YES / UNSURE / NO

6. Vendor Dependency

Does your organization maintain sufficient internal knowledge and control to operate effectively if a major technology vendor or MSP relationship changes?

Strong vendors are valuable partners.

Excessive vendor dependency is different.

Leadership should understand who controls administrative credentials, documentation, configurations, licensing, contracts, backups, and institutional knowledge.

Executive concern: Excessive dependency can reduce negotiating leverage, increase costs, complicate transitions, and create operational risk.

Your Score: YES / UNSURE / NO

SEVENCORE IT STRATEGY GROUP

Executive Brief

7. Backup Readiness

Can leadership verify—not simply assume—that critical business data is backed up, protected, and recoverable?

Having backup software is not the same as having a reliable recovery capability.

Leadership should understand:

- What is being backed up
- What isn't being backed up
- Where backups are stored
- How backups are protected
- How frequently recovery is tested
- How long restoration would take

Executive concern: A backup that cannot be restored when needed provides little business protection.

Your Score: YES / UNSURE / NO

8. Disaster Recovery

Does your organization know how technology operations would be restored following a major outage, cyberattack, natural disaster, or facility disruption?

Disaster recovery requires more than backups.

Organizations need defined priorities, responsibilities, dependencies, recovery procedures, and realistic recovery expectations.

Executives should be able to answer two critical questions:

How quickly must we recover?

How much data can we afford to lose?

Executive concern: Without a tested recovery strategy, the actual cost and duration of a major disruption remain unknown.

SEVENCORE IT STRATEGY GROUP

Executive Brief

Your Score: YES / UNSURE / NO

9. Security Maturity

Can leadership explain the organization's most significant technology risks and the controls in place to manage them?

Cybersecurity maturity isn't measured by the number of security products an organization owns.

It requires understanding the organization's actual exposure.

Leadership visibility should include areas such as:

- Identity and access
- Endpoint protection
- Vulnerability management
- Employee security awareness
- Third-party risk
- Incident response
- Backup protection
- Security policies
- Cyber insurance requirements

Executive concern: Cybersecurity becomes a business risk when leadership lacks visibility into exposure, preparedness, and accountability.

Your Score: YES / UNSURE / NO

10. Leadership Visibility

Does executive leadership receive enough technology information to make informed business decisions?

Executives don't need hundreds of technical metrics.

They need visibility into the issues that affect the business:

- Technology spending
- Major risks

SEVENCORE IT STRATEGY GROUP

Executive Brief

- Infrastructure health
- Cybersecurity exposure
- Vendor performance
- Upcoming investments
- Project priorities
- Business continuity
- Technology roadmap progress

If leadership primarily hears about technology when something breaks or funding is requested, there may be a visibility gap.

Executive concern: Technology becomes reactive rather than strategically managed.

Your Score: YES / UNSURE / NO

CALCULATE YOUR EXECUTIVE IT HEALTH SCORE

Give yourself:

YES = 2 points

UNSURE = 1 point

NO = 0 points

Maximum score: **20**

17–20 | STRATEGICALLY HEALTHY

Your organization demonstrates strong visibility and technology management practices.

The priority should be maintaining that discipline while ensuring your technology strategy continues to align with business growth.

12–16 | ATTENTION RECOMMENDED

Your environment may be operating effectively today, but several areas warrant closer executive review.

Unaddressed gaps can eventually become financial, operational, or security problems.

SEVENCORE IT STRATEGY GROUP

Executive Brief

7–11 | ELEVATED TECHNOLOGY RISK

Multiple indicators suggest that technology risk may not be fully understood or managed.

A structured assessment should be considered to identify priorities before they become larger business issues.

0–6 | EXECUTIVE ACTION RECOMMENDED

Your organization may have significant gaps in technology visibility, resilience, governance, or risk management.

A comprehensive assessment should be prioritized.

PAY PARTICULAR ATTENTION TO "UNSURE"

One of the most important answers on this scorecard is **UNSURE**.

Executives are not expected to know every technical detail of the IT environment.

However, leadership should have enough visibility to understand whether critical technology risks are being identified, managed, funded, and monitored.

When the answer to questions involving backups, cybersecurity, disaster recovery, infrastructure lifecycle, or technology spending is consistently "**I think so**" or "**I'm not sure**," the issue is not necessarily a technology failure.

It is a **visibility and governance gap**.

And that deserves executive attention.

TECHNOLOGY SHOULD SUPPORT THE BUSINESS—NOT SURPRISE IT

A healthy technology environment isn't simply one where everything works today.

It is an environment where leadership understands:

SEVENCORE IT STRATEGY GROUP

Executive Brief

What we have.

What it costs.

Where we're vulnerable.

What needs attention.

What we should invest in next.

That visibility allows organizations to move away from reactive technology decisions and toward deliberate investment, risk management, and strategic planning.

FROM TECHNOLOGY CHAOS TO STRATEGIC CLARITY

SevenCore IT Strategy Group helps organizations evaluate technology through an executive and business lens.

Our **IT Infrastructure Assessment** provides an independent evaluation of the current environment to identify risks, inefficiencies, lifecycle concerns, dependencies, and opportunities for improvement.

The objective isn't to sell your organization more technology.

The objective is to give leadership **clarity about the technology you already have and confidence about what should happen next.**

Schedule a SevenCore IT Infrastructure Assessment

If this scorecard identified several **NO** or **UNSURE** responses, the next step is a structured review of your environment.

SevenCore IT Strategy Group, LLC

Removing Technology Chaos. Creating Strategic Clarity Through Executive IT Leadership.

7corestrategy.com

consulting@7corestrategy.com

SEVENCORE IT STRATEGY GROUP

Executive Brief