LEADERSHIP BRIEF

Cybersecurity Readiness Brief for Leaders and Boards

Twelve practical questions to ask about ownership, provider oversight, insider risk, AI use, and incident readiness, plus a 90-day worksheet to turn the answers into action.

For: Executives, owners, and board members **Edition:** November 2026

Web: spmadvisors.net

ABOUT SPM ADVISORS

Veteran-owned cybersecurity and digital forensics firm helping organizations, healthcare practices, and individuals understand their risk and respond when something goes wrong. Learn more at spmadvisors.net.

INSIDE THIS GUIDE

1. How to use this brief
2. Twelve questions for leadership
3. Scoring the answers
4. 90-day priorities worksheet

How to use this brief

Leaders do not need to be technical to oversee cybersecurity well. They need to ask the right questions, expect clear answers, and make sure someone is accountable for closing the gaps. This brief gives you twelve questions to put to your management team, IT staff, or managed service provider, grouped into five areas that drive most real-world incidents.

- **Ask, then listen for specifics.** Each question includes what a strong answer sounds like and the warning signs that suggest a gap.
- **Score honestly.** Mark each answer as confident, partial, or unknown. "We think so" is unknown.
- **Turn gaps into owned actions.** Use the 90-day worksheet at the end to assign owners, next steps, and dates.

> **THE GOAL**
>
> The goal is not a perfect score. It is a leadership team that knows where it stands, has decided which risks it will accept, and can show progress every quarter.

Twelve questions for leadership

Ownership and governance

1 Who owns cybersecurity risk, and how does it reach this table?

WHY IT MATTERS	When security belongs to "IT" in general, decisions about budget, priorities, and accepted risk get made by default rather than on purpose.
A STRONG ANSWER	A named executive is accountable, a technical lead or provider handles daily operations, and leadership receives a short, regular report covering the same few measures each time.
WARNING SIGNS	"Our IT company handles that." No regular reporting. Security only comes up after a problem.

2 Do we know what we most need to protect, and where it lives?

WHY IT MATTERS	You cannot protect what you have not identified. Most organizations have critical data scattered across email, cloud storage, laptops, and vendor systems.
A STRONG ANSWER	A current list of critical systems and sensitive data (customer, financial, health, employee, intellectual property), where each is stored, and who can reach it.
WARNING SIGNS	No inventory, or one that is years old. Uncertainty about which cloud services staff use.

3 How do we fund security decisions and accept risk?

WHY IT MATTERS Every organization lives with some risk. The problem is risk that nobody consciously accepted.

A STRONG ANSWER Security spending is tied to identified risks. When leadership defers a recommendation, the decision, the reason, and a revisit date are written down.

WARNING SIGNS Budget set as a flat line item with no link to risk. Recommendations that quietly disappear.

Provider and vendor oversight

4 What exactly does our IT or security provider do, and what do they not do?

WHY IT MATTERS Many breaches happen in the space between what the client assumed the provider covered and what the contract actually says.

A STRONG ANSWER A written responsibility matrix covering monitoring, patching, backups, account management, incident response, and after-hours coverage, with each item marked provider, internal, or shared.

WARNING SIGNS "They handle security." A contract nobody has read since signing. No clarity about who responds at 2:00 a.m.

5 How do we verify that the provider is doing it?

WHY IT MATTERS Trust is not oversight. Providers that perform well are usually glad to show evidence.

A STRONG ANSWER Regular reports with evidence: multi-factor authentication coverage, patch status, endpoint protection coverage, backup success and restore tests, and open issues with dates.

WARNING SIGNS Reports that only list tickets closed. No restore test in the past year. Admin accounts shared between provider staff.

6 Which outside vendors hold our data or can access our systems?

WHY IT MATTERS Your exposure includes your vendors' weaknesses. Payroll, billing, software, and support vendors often have broad access.

A STRONG ANSWER A ranked list of key vendors, what data or access each has, contract terms for security and breach notice, and a plan if a critical vendor goes down.

WARNING SIGNS Vendor remote access left always on. No idea which vendors would need to tell you about their breach, or how fast.

Insider risk

7 Who has privileged access, and how quickly is it removed when people leave or change roles?

WHY IT MATTERS Former employees, contractors, and over-permissioned accounts are among the most common paths to data loss, whether intentional or accidental.

A STRONG ANSWER Admin rights are limited and reviewed at least quarterly. HR and IT share a same-day offboarding checklist that covers email, cloud apps, VPN, shared passwords, and company devices.

WARNING SIGNS Shared admin logins. Accounts for people who left months ago. Offboarding that depends on someone remembering.

8 How would we notice misuse by a trusted insider, and how would we handle it fairly?

WHY IT MATTERS Insider incidents are as much about people and process as technology. A poorly handled investigation can create legal and cultural harm.

A STRONG ANSWER Alerts for unusual downloads or forwarding of sensitive data, a clear acceptable-use policy, and a documented process that brings in HR and counsel before anyone confronts an employee or collects evidence.

WARNING SIGNS No visibility into bulk downloads or email forwarding. Managers who would "just look through their computer."

AI use

9 Where are employees using AI tools, and what information goes into them?

WHY IT MATTERS Staff are already using AI assistants, often on personal accounts. Confidential, client, or regulated data pasted into an unapproved tool may be retained or used in ways you cannot control.

A STRONG ANSWER A short, practical AI use policy, a list of approved tools with business accounts and data protections, and clear rules about which information may never be entered.

WARNING SIGNS No policy, or a blanket ban nobody follows. No idea which AI features are switched on inside existing software.

10 What decisions rely on AI output, and how are we protected from AI-enabled fraud?

WHY IT MATTERS AI output can be confidently wrong, and attackers now use convincing voice, video, and writing to impersonate executives and vendors.

A STRONG ANSWER A person reviews AI output before it reaches customers or drives important decisions. Payment and banking changes are always confirmed through a known phone number or second channel, no matter how urgent or convincing the request.

WARNING SIGNS Wire transfers or vendor bank changes approved by email alone. AI-drafted content sent externally without review.

Incident readiness

11 If ransomware hit tomorrow, who decides what in the first 24 hours?

WHY IT MATTERS The first day of an incident is full of decisions with legal, financial, and reputational consequences: whether to shut systems down, whom to call, what to say.

A STRONG ANSWER A written incident response plan naming decision-makers and alternates, with contact details for the insurer, breach counsel, forensic support, and key vendors kept somewhere that works when email and the network do not.

WARNING SIGNS The plan lives only on the server that would be encrypted. Nobody knows the insurer's notice requirements or approved vendors.

12 Can we actually restore our critical systems, and how do we know?

WHY IT MATTERS Backups that have never been tested are hope, not a plan. Attackers routinely target backups first.

A STRONG ANSWER At least one backup copy is isolated from the main network. Restores of critical systems are tested on a schedule, and leadership knows how long recovery would realistically take. A tabletop exercise has been run in the past year.

WARNING SIGNS "The backups run every night" with no restore test. Backups reachable with the same admin password as everything else.

Scoring the answers

Record each answer below. Anything marked partial or unknown becomes a candidate for the 90-day worksheet.

Leadership answer scorecard

#	AREA	CONFIDENT / PARTIAL / UNKNOWN	NOTES
1–3	Ownership and governance		
4–6	Provider and vendor oversight		
7–8	Insider risk		
9–10	AI use		
11–12	Incident readiness		

What to ask for in regular reporting

- Percentage of accounts protected by multi-factor authentication
- Critical patches outstanding beyond target timelines
- Date and result of the last backup restore test
- Open high-risk findings, owners, and due dates
- Incidents and near misses since the last report

Signs the program is maturing

- The same measures are reported each time, with trends
- Deferred risks are documented and revisited
- Provider performance is reviewed against evidence
- Leadership has practiced an incident scenario
- Findings close faster each quarter

90-day priorities worksheet

The suggested priorities below address the gaps we see most often. Keep the ones that match your scorecard, replace the rest, and assign a named owner to each. Owner roles are suggestions; one person can hold several.

90-day priorities, owners, and next actions

PRIORITY	SUGGESTED OWNER	NEXT ACTION	NAMED OWNER / DUE	STATUS
DAYS 1–30: ESTABLISH OWNERSHIP AND VISIBILITY				
Name an accountable executive for cyber risk	CEO / board chair	Assign in writing and set a quarterly reporting date		
Confirm multi-factor authentication everywhere it matters	IT lead / provider	Report coverage for email, remote access, admin, and finance accounts		
Inventory critical systems and sensitive data	Operations / IT lead	One-page list: system, data type, location, owner		
Clarify provider responsibilities	Executive owner	Request a responsibility matrix and current evidence report		
DAYS 31–60: CLOSE THE MOST COMMON GAPS				
Prove backups can be restored	IT lead / provider	Restore one critical system; record time taken and issues		
Review privileged access and offboarding	HR + IT lead	Remove stale accounts; adopt a same-day offboarding checklist		
Adopt an AI use policy	Executive owner + counsel	Approve tools, define prohibited data, communicate to staff		
Lock down payment changes	Finance lead	Require call-back verification for all bank and wire changes		
DAYS 61–90: PRACTICE, MEASURE, AND PLAN AHEAD				
Run a tabletop exercise	Executive owner	Walk leadership through a ransomware scenario; log decisions and gaps		
Update the incident contact sheet	Operations lead	Insurer, counsel, forensics, vendors; store a copy offline		
Rank key vendors by risk	Operations / finance	Top ten vendors: data held, access, breach-notice terms		
Set the reporting format and next-year plan	Executive owner	Adopt standard metrics; schedule an independent assessment		
YOUR ADDITIONAL PRIORITIES				

Status suggestions: Not started, In progress, Done, Deferred (with documented reason and revisit date).

This guide provides general information for planning purposes. It is not legal advice and does not create a client relationship. Requirements and product features change; confirm current details before relying on them. © 2026 SPM Advisors LLC. Edition: November 2026.