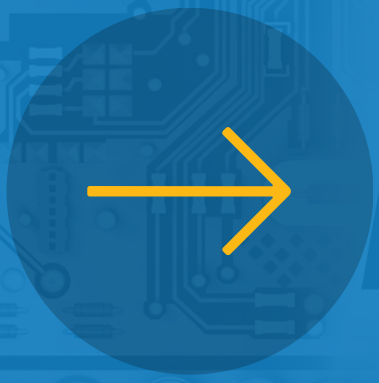
Cyber Risk Readiness Guide

Practical steps to strengthen security, business resilience, and cyber-insurance readiness.



Cyber Risk Is Not Only An IT Issue

A serious incident can interrupt operations, disrupt revenue, expose sensitive information, trigger legal or regulatory obligations, and test whether your insurance and response plans work as expected.

This guide will help executives and technology leaders:

- Identify the controls that matter most
- Ask better questions of IT and insurance advisors
- Evaluate cyber-insurance readiness
- Find consequential gaps that may be easy to overlook
- Build a practical 30-day improvement plan
- Align security decisions with business and insurance priorities

The goal is not zero risk. It is informed risk- understood, prioritized, documented, and managed.



The Executive View of Cyber Risk

Cybersecurity should begin with the business, not the technology. Leaders need to understand critical operations, supporting systems, key data, and the impact of disruption. Proven IT starts by assessing operational context, identity, infrastructure, data, third parties, governance, and incident readiness before building a security roadmap.

NIST's Cybersecurity Framework 2.0 reinforces that cybersecurity requires executive oversight, clear responsibilities, risk-based decisions, and communication—not just security products. Its 2026 guidance also ties cybersecurity risk to enterprise risk management and senior leadership.

Five ways cyber risk reaches the business

1. **Operations:** Systems, communications, production, customer service, billing, or supply chain activities may be interrupted.
2. **Financial performance:** The organization may face recovery costs, lost income, fraud, professional fees, or contractual consequences.
3. **Governance**: Executives may need to demonstrate how risks, responsibilities, exceptions, and investments were evaluated.
4. **Reputation and relationships:** Customers, employees, lenders, partners, and regulators may expect a clear and credible response.
5. **Insurability:** Security controls, documentation, application representations, policy language, and incident procedures must align.

Cyber insurance is an important form of risk transfer, but policies vary significantly. First-party coverage may address certain response, restoration, interruption, extortion, fraud, or crisis-management costs; third-party coverage may address certain claims, litigation, regulatory inquiries, or liabilities. What is included depends on the actual policy, declarations, endorsements, exclusions, limits, and sub limits.

Executive principle

Do not ask only, "Are we secure?" Ask, "What could interrupt the business, how would we detect it, who would make decisions, how would we recover, and what evidence proves our controls operate as represented?"

What “Good” Looks Like and What Evidence to Request

CISA’s Cybersecurity Performance Goals 2.0 prioritize executive oversight, asset management, vulnerability mitigation, MFA, least privilege, segmentation, training, email security, backups, logging, incident communications, and recovery preparedness. The FTC likewise recommends inventories, access control, patching, encryption, backups, monitoring, training, vendor oversight, and tested response plans.

Use the checklist below during a leadership, risk, or technology review.

1. Business-critical operations and assets

Good looks like: IT and business leadership agree on the systems, applications, data, vendors, facilities, and processes that cannot be unavailable beyond an acceptable period.

Request: A current asset inventory, data map, dependency diagram, critical-process list, assigned owners, recovery priorities, and approved recovery objectives.

2. Identity, MFA, and privileged access

Good looks like: MFA is enforced, not merely available, across email, remote access, cloud applications, administrative access, and other sensitive systems. Administrators use separate privileged and everyday accounts. Access is removed promptly when roles change or employment ends.

Request: MFA-enforcement reports, privileged-account inventory, access-review results, inactive-account report, exception list, and recent onboarding/offboarding evidence.

3. Endpoint, network, and cloud protection

Good looks like: Managed laptops, workstations, servers, cloud environments, and internet-facing devices are inventoried, monitored, supported, and protected. Security teams can identify and isolate suspicious devices.

Request: Endpoint protection coverage report, unsupported device list, cloud security findings, network diagram, alert escalation process, and unresolved high-risk exceptions.

4. Vulnerability and patch management

Good looks like: Vulnerabilities are discovered continuously, prioritized according to exploitability and business impact, assigned to owners, remediated, and formally accepted when remediation must be delayed.

Request: Current vulnerability report, patch-compliance dashboard, aging findings, internet-facing exposure report, end-of-life system list, and documented risk acceptances.

5. Email, social engineering, and payment security

Good looks like: Email authentication and filtering are configured; employees can report suspicious messages; and financial requests, vendor banking changes, credentials, and sensitive-data requests require independent verification.

Request: SPF/DKIM/DMARC status, phishing-reporting workflow, training results, payment-change procedure, and evidence that high-risk transactions require out-of-band confirmation. The FBI specifically recommends independently verifying payment or account changes and resisting urgent requests.

6. Backups and recovery

Good looks like: Critical systems and data are covered by backups resilient to compromise. Restoration, not merely backup completion, is tested against approved recovery priorities.

Request: Backup scope, failed-job report, access controls, isolation or immutability settings, latest restore-test results, achieved recovery times, and open corrective actions.

7. Monitoring and detection

Good looks like: Important identity, endpoint, network, cloud, email, and administrative events are collected, reviewed, and escalated to named responders.

Request: Log-source inventory, retention settings, alert ownership, after-hours escalation procedure, sample incident tickets, and metrics for unresolved security alerts.

8. People, vendors, data, and response

Good looks like: Employees receive role-relevant training; vendors are risk-tiered and access only what they need; sensitive data is limited, encrypted, retained appropriately, and disposed of securely; and the incident plan is exercised with executives, IT, legal, communications, and insurance contacts.

Request: Training completion, vendor access report, key contract requirements, data retention schedule, incident plan, tabletop report, contact tree, and remediation tracker.



Can You Prove What Your Application Says?

Score each statement:

0 - No: The control is absent or unknown

1 - Partial: It exists, but coverage, ownership, testing, or evidence is incomplete

2 - Validated: It is operating across the defined scope and current evidence is available.

Readiness Area	Score
Critical operations, systems, data, and dependencies are documented	/ 2
MFA and privileged-access controls are validated across the stated scope	/ 2
Endpoint protection, monitoring, and escalation are operational	/ 2
Vulnerability and patch management produce current evidence	/ 2
Backups cover critical assets and restorations are tested	/ 2
Email, payment, and social-engineering controls are documented	/ 2
Employee training and reporting procedures are active	/ 2
Vendor access and third-party cyber risk are reviewed	/ 2
Incident response is current, exercised, and insurance-aware	/ 2
Application answers and policy requirements have been reviewed jointly by IT and the broker	/ 2
TOTAL	/ 20

How to interpret your score

18–20: Evidence-ready. Confirm that evidence is current and policy-specific.

10–15: Partially ready. Prioritize gaps that affect critical operations or application representations.

0–9: Material uncertainty. Conduct a structured assessment before making or renewing representations.

Important

This is a management triage tool, not an underwriting model. A score does not predict availability, pricing, limits, exclusions, or claim outcomes. Those decisions vary by insurer, policy, organization, jurisdiction, industry, and incident.

Readiness Rule

A “yes” should mean: implemented, correctly scoped, operating, owned, periodically reviewed, and supported by evidence.



The Gaps Between the Tools

MFA that does not cover every important access path

Why it matters: MFA on email but not remote access, administrative accounts, cloud consoles, vendors, or legacy systems can leave a consequential opening.

Recognize it: IT reports that MFA is “enabled” but cannot produce an enforcement or exception report.

Corrective action: Define the required scope, validate enforcement, remove unnecessary exceptions, and strengthen authentication for executives and privileged users.

Backups that have never been restored

Why it matters: A successful backup job does not prove that data, applications, configurations, and dependencies can be restored in the required order.

Recognize it: Reports show backup completion but no dated restoration results or achieved recovery times.

Corrective action: Test a business-relevant restoration, record what failed, and assign corrective actions.

An incident plan that exists only on paper

Why it matters: An untested plan may contain outdated contacts, unclear authority, unavailable vendors, or steps that conflict with policy notification and consent requirements. Proven IT identifies lack of testing, unclear ownership, weak escalation, inadequate communication, and limited executive involvement as common response gaps.

Corrective action: Run a tabletop using ransomware, business email compromise, or a major vendor outage.

Payment controls that trust email, voice, or video

Why it matters: AI can make phishing, voice cloning, and video impersonation more convincing. The FBI recommends treating urgent requests for money or credentials cautiously, educating employees, using MFA, and verifying sensitive or financial requests through trusted channels.

Corrective action: Require independent verification for new payees, banking changes, unusual payments, password resets, sensitive records, and executive requests, regardless of how authentic the communication appears.

Third-party access without clear ownership

Why it matters: Vendors may hold data, administer systems, connect remotely, or support critical operations.

Recognize it: No single inventory shows vendor access, data handled, business dependency, security obligations, or incident-notification contacts.

Corrective action: Tier vendors by impact, restrict access, require MFA, document security and reporting obligations, and verify compliance.

Security evidence assembled only at renewal

Why it matters: Last-minute evidence may reveal that a control is partial, a report is outdated, or the application language does not match actual operation.

Corrective action: Maintain an annual evidence file containing control owners, policy exports, coverage reports, restore tests, tabletop records, training completion, risk exceptions, and remediation status.

Ask for Answers You Can Evaluate

1. Which business processes would hurt us most if they stopped tomorrow?

A strong answer includes: Revenue, payroll, customer service, operations, safety, contractual commitments, critical applications, data, vendors, and recovery priorities.

Red flag: A list of servers without business impact or ownership.

2. What are our three most material cyber risks?

A strong answer includes: Scenario, affected operation, likelihood, consequence, current controls, residual risk, owner, next action, and target date.

Red flag: "Ransomware" or "phishing" without explaining exposure or business impact.

3. Where is MFA enforced, and where is it not?

A strong answer includes: Email, VPN, remote access, administrators, cloud platforms, vendors, exceptions, legacy protocols, and remediation plans.

Red flag: "We have MFA" with no coverage report.

4. Can we account for every device, application, administrator, and internet-facing system?

A strong answer includes: Reconciled inventories, assigned owners, supported status, vulnerability visibility, and a process for discovering unknown assets.

Red flag: Separate lists that disagree or omit cloud and vendor-managed systems.

5. Which vulnerabilities remain unresolved beyond our target?

A strong answer includes: Severity, exploitability, internet exposure, affected business process, compensating controls, owner, and approved exception.

Red flag: A scan containing thousands of findings but no prioritization or accountability.

6. Could we restore our most critical operation from clean backups?

A strong answer includes: What was restored, when it was tested, who participated, achieved recovery time, missing dependencies, and corrective actions.

Red flag: "The backup dashboard is green."

7. Who monitors our environment after hours, and what happens when an alert appears?

A strong answer includes: Covered systems, who receives alerts, severity criteria, escalation path, containment authority, and executive-notification thresholds.

Red flag: Tools generate alerts, but responsibility between employees and providers is unclear.

8. How would we respond if an executive's email or voice appeared to authorize a payment?

A strong answer includes: Independent verification, dual authorization, trusted callback information, finance escalation, account containment, and rapid contact with financial institutions.

Red flag: Employees are expected to judge authenticity from writing style, caller ID, or video appearance.

9. When did we last test our incident-response plan?

A strong answer includes: Scenario, participating functions, decisions tested, gaps found, lessons learned, and remediation status. NIST's 2025 incident-response guidance integrates preparation and continuous improvement across the full risk-management lifecycle.

Red flag: The plan was updated, but no exercise was conducted.

10. Which vendors create the greatest concentration or access risk?

A strong answer includes: Critical service dependencies, data access, remote privileges, alternative procedures, contractual notification requirements, and exit or continuity options.

Red flag: Vendor risk is treated only as procurement paperwork.

11. Can we prove the statements made on our insurance application?

A strong answer includes: A mapping from every technical statement to an owner, configuration, report, test result, exception, and review date.

Red flag: Finance or the broker completed technical answers without IT validation.

12. What do you need from leadership?

A strong answer includes: Prioritized decisions involving risk acceptance, funding, staffing, business participation, policy enforcement, vendor accountability, and recovery requirements.

Red flag: Every security problem is framed as a request for another product.

Understand the Cyber Policy Before You Need It

Cyber policies are customized, and similar terms may produce different results across forms and endorsements. Ask your licensed broker and qualified counsel to explain the policy in the context of your organization.

1. What events trigger each major coverage section?

Clarify network security, privacy, data restoration, incident response, business interruption, contingent interruption, cyber extortion, computer fraud, social engineering, funds-transfer fraud, regulatory proceedings, and media exposure.

2. What are the limits, sublimits, retentions, and waiting periods?

Ask for a simple schedule showing how much is available, what the organization pays or absorbs, and whether time-based waiting provisions apply.

3. How are business interruption and contingent business interruption calculated?

Clarify covered systems, dependent vendors, required proof, waiting-period mechanics, period of restoration, and treatment of extra expense.

4. How does the policy address social engineering, invoice manipulation, executive impersonation, and funds-transfer fraud?

Determine whether these risks have separate insuring agreements, sublimits, verification conditions, or exclusions. Travelers, for example, publishes separate social-engineering supplements, illustrating why leaders should not assume fraud coverages are identical.

5. Which exclusions deserve executive attention?

Ask specifically about prior knowledge, contractual liability, failure to maintain controls, infrastructure or utility failures, acts of war, systemic events, insider conduct, unencrypted devices, regulatory matters, and collection or use of data.

6. Exactly when and how must we report a suspected incident?

Obtain the hotline, email, policy number, broker escalation contact, required information, and definitions of incident, claim, discovery, and notice.

7. Must we use panel vendors or obtain consent before incurring costs?

Clarify which breach counsel, forensic investigators, notification providers, crisis communications, negotiators, restoration specialists, and accountants are approved. Carrier panels can include distinct providers for legal, forensics, notification, PR, deepfake analysis, and financial-loss documentation.

8. What incident-response resources are available before and after an event?

Ask about hotlines, breach coaching, tabletop support, risk scans, pre-claim assistance, forensic services, and claims advocacy.

9. How were our limits selected?

Connect limits to organization-specific interruption scenarios, revenue dependency, sensitive-record exposure, fraud authority, vendor concentration, recovery costs, and legal obligations, not a generic industry average.

10. Which application statements become material to underwriting or coverage?

Before signing, have IT validate technical answers and document qualifications or exceptions.

11. How could business changes affect the policy?

Discuss acquisitions, new locations, cloud migrations, AI adoption, new payment processes, regulated data, operational technology, outsourcing, and critical vendors.

12. What should IT, leadership, legal, and the broker review together before renewal?

Request a structured pre-renewal meeting rather than exchanging forms by email.



The 30-Day Readiness Plan

Days 1–7: Establish the business view

- ☐ Name an executive sponsor and an accountable security leader.
- ☐ Identify the five to ten processes most important to revenue, service, operations, safety, or legal obligations.
- ☐ Map their systems, data, administrators, vendors, and recovery dependencies.
- ☐ Gather the current insurance policy, endorsements, application, incident contacts, and renewal date.

Days 8–14: Validate high-impact controls

- ☐ Review MFA coverage and privileged accounts.
- ☐ Reconcile asset, endpoint, and administrative-account inventories.
- ☐ Review unresolved internet-facing vulnerabilities and unsupported systems.
- ☐ Confirm endpoint monitoring and after-hours escalation.
- ☐ Examine email-authentication and financial-verification procedures.

Days 15–21: Test resilience

- ☐ Perform a restore test for one critical process.
- ☐ Review incident-response contacts and decision authority.
- ☐ Run a tabletop involving leadership, IT, finance, operations, legal, communications, and the broker.
- ☐ Record gaps, owners, decisions, and deadlines.

Days 22–30: Align technology and insurance

- ☐ Compare actual controls with application representations.
- ☐ Review limits, sublimits, retentions, exclusions, waiting periods, notification procedures, and panel-vendor requirements.
- ☐ Correct inaccurate documentation.
- ☐ Prioritize remaining gaps by business impact.
- ☐ Approve a 90-day remediation roadmap and define how progress will be tracked and verified.

Build Readiness Before It Becomes an Emergency

Cyber resilience doesn't come from a single product, policy, or annual form. It comes from understanding the business, validating controls, testing responses, documenting evidence, and aligning security and insurance decisions.

Proven IT's enterprise materials describe capabilities that include cybersecurity assessment, vulnerability management, monitoring, backup and disaster recovery, incident-response planning, strategic guidance, and fractional security leadership. Its incident-response approach includes capability assessment, environment-specific procedures, monitoring, supporting technologies, and response playbooks.

Schedule a Cybersecurity Consultation with Proven IT

A conversation with Proven IT can help your leadership and IT teams:

- **Clarify business-critical cyber risks**
- **Identify gaps requiring deeper assessment**
- **Review incident-response and recovery readiness**
- **Connect security priorities to business impact**
- **Build a practical, prioritized path forward**

Schedule My Cybersecurity Consultation

Disclaimer: *This guide provides general educational information and is not legal, insurance, regulatory, audit, or compliance advice. Coverage and underwriting requirements vary. Consult qualified cybersecurity, insurance, legal, and regulatory professionals regarding your organization and policy.*