SECURITY CHECKLIST

Cybersecurity Readiness Checklist

A leadership-level checklist for reducing exposure across identity, endpoints, email, backups, vendors, users, monitoring, and incident response.

WHITEPAPER 04

BUILT FOR

Business owners, executives, IT leaders, compliance owners, and organizations preparing for cyber insurance, audits, or growth.

OUTCOME

A practical security baseline that helps leadership understand what is working, what is missing, and what needs priority attention.

USE THIS WHEN

Leadership needs a practical security baseline for risk reviews, cyber insurance, audits, or board-level visibility.

WHY THIS WHITEPAPER MATTERS

Executive brief

Cybersecurity readiness is not the same as buying tools. Mature organizations know who has access, what devices exist, which systems matter, how alerts are reviewed, whether backups recover, and what happens during an incident. This checklist turns security into a clear operating discipline.

Business continuity

Ransomware, credential theft, data loss, and system outages can stop operations, billing, service delivery, and communications.

Regulatory exposure

Healthcare, finance, payment, and public sector environments often have formal safeguard, privacy, or evidence expectations.

Insurance pressure

Cyber-insurance applications increasingly ask specific questions about MFA, backups, EDR, patching, access, training, and incident response.

Leadership accountability

Executives need a prioritized risk picture, not scattered tool screenshots.

Leadership takeaway: Cybersecurity readiness is an operating discipline that connects identity, endpoint, email, backup, monitoring, policy, and response.

COMMON FAILURE PATTERNS

Where organizations lose control

Security risk grows when basic controls are incomplete, unverified, or split across owners with no shared evidence.

What to watch for

- MFA is enabled for some users but not enforced consistently across email, remote access, admin accounts, and cloud apps.
- Endpoints are protected, but coverage gaps exist for old devices, remote users, servers, or personally assigned equipment.
- Backups exist but are not regularly tested for restoration, ransomware resilience, retention, and recovery time.
- Administrators use shared accounts, excessive permissions, stale access, or unmanaged vendor credentials.
- Security alerts are generated but not owned, reviewed, escalated, and documented.
- The incident response plan exists as a file, not as a rehearsed operational process.

Operational truth: Security control is not a product count. It is the ability to prove coverage, ownership, monitoring, response, and recovery.

Impact if ignored

Small gaps become recurring tickets, missed handoffs, delayed projects, unclear security ownership, and leadership surprises.

Corrective move

Assign an owner, define the standard, require evidence, and review progress on a leadership cadence.

OPERATING MODEL

The Practical Cybersecurity Baseline

A mature approach turns scattered activity into a repeatable system. Use this model to define ownership, sequence, quality checks, and handoff.

1

Identify

Know assets, users, critical systems, data flows, vendors, dependencies, and business impact.

2

Protect

Apply MFA, least privilege, endpoint protection, patching, secure configuration, backup controls, and user safeguards.

3

Detect

Monitor endpoints, identities, email, critical logs, suspicious behavior, and high-risk changes.

4

Respond

Define roles, escalation, containment, communications, evidence handling, and decision authority.

5

Recover

Validate backups, restore priorities, recovery objectives, post-incident lessons, and business continuity actions.

Execution rule: Do not move from one stage to the next until ownership, evidence, and acceptance criteria are clear.

01

Own the standard

Decide what good looks like before work begins.

02

Prove readiness

Verify facts before scheduling, buying, deploying, or closing.

03

Close the loop

Document outcomes so support and leadership can act.

STANDARDS THAT MAKE THE WORK REPEATABLE

What good looks like

A professional IT program does not rely on memory or individual heroics. It uses standards that make quality visible, measurable, and repeatable.

Standard area	Practical expectation
Identity security	MFA, conditional access, privileged account control, stale-account removal, vendor access review.
Endpoint security	EDR/MDR coverage, encryption, patching, device inventory, remote wipe, standard builds, local admin control.
Email security	Phishing controls, domain protection, user training, reporting process, suspicious message review.
Backup resilience	Immutable or protected backups where appropriate, restore tests, retention policy, documented recovery priorities.
Incident readiness	Playbooks, contact list, escalation rules, legal/insurance notification pathway, tabletop exercises.

Decision principle: Anything that cannot be documented, repeated, assigned, measured, or handed off will eventually become support debt.

Documented

The process is written and current.

Measured

Leadership can see trend and risk.

Owned

Someone is accountable for completion.

ACTIONS THAT CREATE REAL PROGRESS

Implementation playbook

Use these actions to move from vague concern to a practical operating plan. Each item should have an owner, due date, and evidence of completion.

- ✓ Start with identity and access because stolen credentials are a common path into business systems.
- ✓ Test restoration from backup before assuming the business can recover.
- ✓ Review administrator, vendor, and service accounts on a recurring schedule.
- ✓ Use leadership reporting that shows risk, gaps, progress, and decisions needed.
- ✓ Measure endpoint coverage by actual device inventory, not by purchased licenses.
- ✓ Document business-critical systems and decide restoration priority before an incident.
- ✓ Build a simple incident response plan that names decision-makers and actions, not just theory.

Practical priority: Fix the facts first. Most technology programs improve faster once inventory, ownership, access, documentation, and acceptance criteria are clean.

HOW LEADERSHIP SHOULD TRACK IT

Governance and measurement

The right metrics make progress visible. The wrong metrics make a messy environment look busy. Leadership should track the signals that explain health, risk, and accountability.

Measurement area	What to track
Identity	MFA coverage, admin account count, stale account count, privileged access review completion.
Endpoint	EDR coverage, encryption coverage, patch compliance, unsupported OS/device count.
Backup	Successful backup rate, restore test frequency, recovery point/time objective fit, backup isolation.
Detection	Alert review time, escalated event count, unresolved high-risk alerts, log source coverage.
Response	Tabletop completion, playbook freshness, contact list accuracy, incident lessons closed.

Reporting rule: A leadership report should answer four questions: What changed? What risk remains? What decision is needed? What happens next?

Executive view

Show the top risks, blocked work, cost impact, and decisions due.

Operational view

Show work volume, aging, recurring issues, defects, and ownership.

USE THESE BEFORE APPROVAL

Executive decision questions

These questions are designed to expose weak assumptions before they become project delays, support issues, security gaps, budget surprises, or operational risk.

- ✓ Is MFA enforced for all users, admins, remote access, email, and critical cloud systems?
- ✓ Can we prove backups restore the systems that matter most?
- ✓ Are vendors and service accounts reviewed for access and necessity?
- ✓ What security evidence can we produce for insurance, audit, or customer requests?
- ✓ Do we know every endpoint, server, mobile device, and unmanaged device in the environment?
- ✓ Who can approve containment, shutdown, legal notice, customer communication, and vendor escalation?
- ✓ How fast are critical alerts reviewed, and who owns escalation?
- ✓ What are the top five risks leadership needs to fund or accept?

What strong answers sound like

Strong answers include ownership, current state, target state, evidence, tradeoffs, timing, dependencies, and the decision leadership needs to make.

SCORE HONESTLY BEFORE INVESTING

Readiness scorecard

Rate each area from 1 to 5. A score of 1 means ad hoc and risky. A score of 3 means partially controlled. A score of 5 means documented, measured, reviewed, and repeatable.

1. **Identity hardening**
   MFA, least privilege, and access reviews are enforced and documented.
2. **Endpoint control**
   Devices are inventoried, protected, patched, encrypted, and supportable.
3. **Backup readiness**
   Backups are protected, monitored, and tested against real recovery needs.
4. **Detection maturity**
   Alerts are reviewed, triaged, escalated, and tied to response actions.
5. **Incident response**
   Roles, decisions, communications, containment, and recovery are rehearsed.
6. **Governance**
   Leadership receives clear reporting and makes risk-based decisions.

Scoring rule: The overall score is not the average. The weakest critical area usually defines the real risk.

TURN THE GUIDE INTO MOVEMENT

30/60/90 action plan

A useful whitepaper should turn into execution. This plan gives leadership a practical starting point for improving control without overcomplicating the first step.

Days 1-30	Days 31-60	Days 61-90
Validate MFA, admin accounts, endpoint coverage, backup status, critical systems, and security tool ownership.	Close high-risk identity gaps, improve endpoint/patch coverage, test restores, and draft incident roles.	Run a tabletop, finalize playbooks, create leadership dashboard, and build the next risk-reduction roadmap.

How HTG applies this in the real world

HTG helps organizations turn technology priorities into executable work: assessments, procurement, staging, managed services, cybersecurity readiness, lifecycle visibility, field execution, infrastructure projects, and leadership reporting.

Ready to turn this into a practical operating plan?

Use this guide as the starting point for a focused review of your environment, risk, priorities, projects, and next decisions.

TALK WITH HTG

ACCURACY AND PRACTICAL USE

Source-grounded notes and reference basis

This whitepaper is written for executive planning and practical operations. It uses recognized public guidance as a foundation where security, continuity, privacy, data protection, incident response, media sanitization, healthcare, financial safeguards, or payment security concepts are discussed.

- **NIST CSF 2.0:** National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29, February 2024. https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final
- **CISA CPG 2.0:** Cybersecurity and Infrastructure Security Agency, Cross-Sector Cybersecurity Performance Goals 2.0. https://www.cisa.gov/cybersecurity-performance-goals-2-0-cpg-2-0
- **CIS Controls v8.1:** Center for Internet Security, CIS Critical Security Controls Version 8.1. https://www.cisecurity.org/controls/v8-1
- **NIST IR:** National Institute of Standards and Technology, SP 800-61 Rev. 3, Incident Response Recommendations and Considerations. https://csrc.nist.gov/pubs/sp/800/61/r3/final
- **NIST Contingency:** National Institute of Standards and Technology, SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems. https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final

Important: This guide is business guidance, not legal, compliance, insurance, or audit advice. Requirements vary by environment, contract, industry, cyber-insurance policy, and regulator. Use it to improve planning, then confirm obligations with the appropriate counsel, auditor, carrier, or compliance owner.

HTG closing standard

The best technology work is not merely installed. It is documented, governed, supported, measured, and improved.