Checklist

SHADOWHQ

Cyber Incident Readiness Checklist

Is your organization truly ready to respond and recover fast when cyberattacks strike?

This quick-reference checklist helps security leaders evaluate incident preparedness across five core areas of cyber resilience. Use it to identify gaps, prioritize improvements, and align your response strategy to modern threats.

How to use the checklist:

For each question, assign yourself a score based on your current capabilities:

- **2** – Yes: we have this in place
- **1** – Somewhat: We're working on it or it's partially implemented
- **0** – No: We do not have this in place

Response Planning & Playbooks

Objective:
Ensure your team has documented, accessible, and actionable plans for top risk scenarios.

- [0] [1] [2] Response playbooks are developed for key threats (e.g., ransomware, insider threat, BEC)
- [0] [1] [2] Playbooks map clearly to business impact and technical actions
- [0] [1] [2] Playbooks are stored in a secure, out-of-band location — accessible even when primary systems are down
- [0] [1] [2] Each task is assigned a clear owner and estimated time to completion
- [0] [1] [2] Roles and responsibilities are cross-functional and defined
- [0] [1] [2] Playbooks are reviewed and updated regularly

Pro Tip: *Storing playbooks in ShadowHQ ensures 24/7 access during active incidents — even if email or SSO are compromised.*

Tabletop Exercises & Testing

Objective:
Test your organization's ability to execute under real-world conditions.

- [ ] 0 1 2 A tabletop exercise was conducted in the last 12 months
- [ ] 0 1 2 Executive, legal, comms, and IT teams participated
- [ ] 0 1 2 The exercise simulated degraded conditions (e.g., email or tooling compromise)
- [ ] 0 1 2 Lessons learned were documented and tracked to closure
- [ ] 0 1 2 A recurring tabletop schedule or testing calendar is in place

Pro Tip: *Run pressure-tested exercises using ShadowHQ to simulate realistic command-and-control challenges.*

Communications & Coordination

Objective:
Ensure secure, clear communication across teams when crisis hits.

- [ ] 0 1 2 Out-of-band communication platform is in place (e.g., ShadowHQ)
- [ ] 0 1 2 Pre-approved templates exist for internal, external, and regulatory messaging
- [ ] 0 1 2 Contact lists for all key stakeholders are up-to-date and tested
- [ ] 0 1 2 Teams are trained to escalate and activate incident communications
- [ ] 0 1 2 Call-tree or mass-notification systems are integrated and tested regularly

Pro Tip: *With ShadowHQ, your team can communicate securely and coordinate response — even when core systems are compromised.*

Gap Management & Resilience Optimization

Objective:
Drive continuous improvement and track measurable resilience progress.

- [ ] 0 1 2 A formal incident response gap assessment was conducted in the last 12 months
- [ ] 0 1 2 Gaps are tracked, prioritized, and assigned owners
- [ ] 0 1 2 Follow-through is measured in a centralized dashboard or system
- [ ] 0 1 2 Gaps from past incidents and exercises are captured and addressed
- [ ] 0 1 2 A cyber resilience backlog or roadmap exists and evolves with testing

Pro Tip: *ShadowHQ helps track and close gaps with built-in dashboards and action management.*

Certification & Incident Governance

Objective:
Align cyber readiness to industry standards and ensure executive visibility.

- [ ] 0 1 2 Your incident response plan has been externally reviewed or certified
- [ ] 0 1 2 Readiness aligns with frameworks like NIST, ISO 27001, or SOC 2
- [ ] 0 1 2 The board or senior leaders are briefed on cyber posture regularly
- [ ] 0 1 2 Audit trails are maintained for IR plan changes, access, and testing
- [ ] 0 1 2 A governance function is assigned to oversee readiness initiatives

Pro Tip: *ShadowHQ makes it easy to brief executives and document governance progress with automated reporting.*

Scoring & Readiness Band

Tally your points and see get your incident preparedness grade:

Score	Readiness Level
0-15	**High Risk** - Immediate action required
15-25	**Low-Medium Risk** - Strengthen and optimize
26-52	**Cyber Resilient** - Proven readiness

ShadowHQ was built for these moments.

When core systems go dark, ShadowHQ keeps your team connected, coordinated, and in control — securely and out-of-band.

Want a deeper view into your incident readiness posture?
Schedule a demo to see how ShadowHQ can help your team modernize and secure cyber crisis management.

Book a Demo

SHADOWHQ

Go from breach to containment faster with ShadowHQ

ShadowHQ is a secure, out-of-band platform that helps CISOs and disaster recovery teams achieve incident preparedness.
Learn more at **www.shadowhq.io**