CENOVA CYBER
MANAGED SECURITY SERVICES

www.cenovacyber.com

Executive Cybersecurity Checklist

A Practical Guide for Business Leaders

Cybersecurity is no longer an IT issue—it's a business risk, financial risk, and leadership responsibility. This checklist helps executives quickly assess whether their organization has the visibility, governance, and accountability needed to manage cybersecurity risk effectively.

---

1. Leadership & Accountability

☐ Is cybersecurity risk discussed at the **executive or board level** at least annually?
☐ Is there a **single accountable security leader** (CISO or vCISO)?
☐ Do executives clearly understand **who owns cyber risk decisions**?
☐ Is cybersecurity integrated into **business strategy and budgeting**?

✅ *If not, your organization may lack executive-level cybersecurity governance.*

2. Risk Visibility & Business Impact

☐ Do we know our **top 5 cyber risks** in business terms (financial, operational, reputational)?
☐ Have we identified our **most critical systems, data, and vendors**?
☐ Is cyber risk **measured and tracked**, not guessed?
☐ Do leaders receive **regular risk reporting**, not just technical metrics?

✅ *Executives should understand cyber risk the same way they understand financial risk.*

3. Compliance & Regulatory Readiness

☐ Do we know which **regulations or frameworks apply** to us (HIPAA, SOC 2, CMMC, PCI, NIST, etc.)?
☐ Are policies documented, current, and aligned to actual operations?
☐ Have we been assessed against relevant standards in the last 12–18 months?
☐ Can we confidently defend our security posture to auditors or customers today?

✅ *Compliance failures often signal deeper security leadership gaps.*

4. Cyber Insurance Preparedness

☐ Has leadership reviewed our **cyber insurance coverage and exclusions**?
☐ Would we pass a **cyber insurance questionnaire today**?
☐ Are our controls actively implemented—not just written down?
☐ Do we understand how a claim could be denied?

✅ *Insurance requires proof—not promises.*

5. Incident Response & Crisis Leadership

☐ Do we have a **documented incident response plan**?
☐ Has leadership reviewed or exercised the plan?
☐ Do we know **who makes decisions during a cyber incident**?
☐ Are legal, communications, and executive roles clearly defined?

✅ *During an incident, confusion is more damaging than the attack itself.*

6. Vendor & Third-Party Risk

☐ Do we assess the security of **critical vendors and service providers**?
☐ Are vendor risks prioritized based on access to data or systems?
☐ Is third-party risk reviewed regularly—not once and forgotten?

✅ *You inherit the cyber risk of your vendors.*

7. Alignment Between IT, Security, and Leadership

☐ Can leadership clearly explain the organization's cybersecurity strategy?
☐ Do IT and security teams understand business priorities and constraints?
☐ Are security decisions made intentionally—not reactively?

✅ *The biggest risk is misalignment between technology and leadership.*

8. Security Leadership Model

☐ Do we have dedicated **security leadership**, not just technical oversight?
☐ Is someone responsible for **strategy, governance, and accountability**—not only tools?
☐ Would a **virtual CISO (vCISO)** model provide the clarity and leadership we need without full-time cost?

✅ *Security leadership is about direction, not just defense.*

Executive Takeaway

If you checked **"No"** or **"Unsure"** in multiple areas, your organization may be:

- Underestimating cyber risk
- Over-relying on tools without strategy
- Missing executive-level security leadership

Modern organizations increasingly address this gap through **Virtual CISO (vCISO) services**—providing experienced cybersecurity leadership aligned to business goals without the cost of a full-time executive.

Learn more about Cenova Cyber's vCISO services
https://www.cenovacyber.com/vciso