Cybersecurity Tabletop Exercise Guide

This is designed to help CFOs at growth-stage companies facilitate and prepare for a cybersecurity tabletop exercise. The objective is to simulate a ransomware or data breach incident and assess the company's readiness from a financial, legal, operational, and reputational standpoint.

📍 When and How to Run Tabletop Exercises

- **At your annual or semi-annual leadership offsite (in-person):**
  This is the best environment for cross-functional alignment, especially when you include the CEO, CISO, general counsel, comms lead, and CFO.
- **As a virtual 90-minute tabletop once per year (if distributed):**
  Better than nothing. Use scenario-based facilitation to test decision-making, communications, and escalation paths.
- **Within 30 days of key changes:**
  If you've just gone through a leadership transition, M&A activity, infrastructure overhaul, or cybersecurity incident, consider running an ad-hoc exercise.

🕑 How Much Time Should Be Carved Out?

- **60–90 minutes** for a basic, single-scenario tabletop
- **2–3 hours** for a more comprehensive cross-functional session
- **Add 30 minutes** for debriefing and documenting lessons learned

1. Assemble the Right Team

Include leaders from:

- Finance (CFO + Controller)
- Legal (GC or outside counsel)
- IT/Security (CISO or head of engineering)
- HR (for insider threats)
- Communications (for internal/external messaging)
- CEO and/or board representative

2. Define the Scenario

Choose a scenario that is relevant and challenging:

- **Ransomware attack** on production environment
- **Credential stuffing** leading to financial fraud
- **Insider leak** of sensitive IP or customer data
- **Deepfake voice attack** triggering a fraudulent wire transfer

Provide a timeline of how the incident unfolds (e.g. discovery at 10am, data exfiltration confirmed by 12pm, ransom demand by 2pm).

3. Facilitate the Discussion

Use a moderator (can be internal or a consultant) to walk through the scenario:

- **Financial Response:** Do we have a retainer or budget for incident response? Would we pay a ransom? Do we know how to transfer crypto funds legally?
- **Insurance:** Are we covered for this type of incident? What preconditions apply?
- **Regulatory:** Would this trigger SEC or GDPR reporting thresholds? Who decides materiality?
- **Board Involvement:** How and when would we loop them in? Is it documented in minutes?
- **Customer Communication:** Who signs off on breach notifications? How fast? Who is the voice / spokesperson / sender?

4. Capture Gaps & Next Steps

Conclude the session by identifying:

- Unclear decision paths
- Missing documentation or policies
- Delays in response coordination
- Training needs (e.g. on crypto transactions or breach disclosure law)

Assign owners and set deadlines for each follow-up.

5. Report Back to the Board

Summarize:

- What went well
- What gaps were found
- What actions will be taken

Document the exercise in your audit committee minutes to demonstrate governance and risk management.