Cybersecurity Playbook for CFOs

Introduction

As a CFO, you play a critical role in safeguarding your company's financial resilience, including navigating the complexities of cybersecurity.

This playbook is designed to provide you with actionable steps to enhance your organization's cybersecurity posture, specifically tailored for growth-stage companies. It combines strategic insights with a practical assessment tool to help you prioritize and implement necessary changes.

10 Moves to Make Before Your Next Cybersecurity Incident

These moves will help protect your company's balance sheet, brand, and board by proactively addressing cybersecurity risks.

1. **Own Your Role in Cybersecurity Governance**
    - Be an active risk manager and drive cybersecurity strategy discussions.
    - Ensure security spending is tied to measurable risk reduction.
    - Incorporate cybersecurity updates in Audit Committee meetings and document discussions in board minutes.

2. **Launch a Tabletop Exercise for Incident Response**
    - Conduct simulation drills for ransomware and breach scenarios with leadership.
    - Plan for ransom payment scenarios.
    - Establish insurance, law firm, and forensic partnerships.

3. **Master the Basics: Cyber Hygiene is Non-Negotiable**
    - Work with your IT organization on a concrete plan and process for patching operating systems, phones, and browsers aggressively—even if it feels tedious. Missed patches and updates are the #1 cause of avoidable breaches, lasting years beyond vulnerability disclosures.
    - Enforce mobile device management (MDM) on BYOD devices.

4. **Benchmark Your Security Posture (Before You Have To)**
    - Conduct proactive security assessments using insurance carriers or third-party experts.
    - Link findings to specific risk reduction actions.
    - Utilize cyber insurance underwriters' evaluations as indicators of vulnerabilities.

5. **Prepare for AI-Driven Attacks**
    - Acknowledge and communicate the increased threat level due to AI-powered cybercrime.
    - Train employees to recognize deep fakes, phishing, and AI-powered fraud.
    - Use "safe words" or verbal passwords for financial transactions taking place over Zoom or phone.

6. **Govern Internal AI Use**
    - Develop and document clear AI use policies for employees.
    - Implement compliance tools for monitoring data sharing with AI platforms.
    - Focus on good governance to protect the board from liability.

7. **Slim Down Your Cybersecurity Stack**
    - More tools ≠ more protection. Avoid security tool bloat and overlapping systems.
    - Challenge every new tool purchase: "Is this reducing material risk, or creating noise?"
    - Outsource intelligently — don’t try to build an elite cybersecurity team internally.

8. **Treat Cyber Insurance as a Strategic Tool, Not a Checkbox**
    - Focus on catastrophic loss protection rather than day-to-day risks.
    - Regularly review insurance limits and coverage terms.
    - Be wary of “double-paying” for retainer services that insurance may already cover after an incident.

9. **Extend Your Risk Lens to Third Parties**
    - Assess cybersecurity practices and insurance of cloud providers, contractors, and vendors.
    - Ensure third parties have adequate cyber risk insurance.

10. **Build a Risk Committee with Cross-Functional Leaders**
    - Establish a Risk Committee with CISO, General Counsel, HR, and yourself.
    - Prioritize ongoing risk identification—not just compliance checklists.
    - Workforce behavior (insiders) remains the greatest cyber threat; HR should always have a seat at the table.

Cybersecurity Readiness Scorecard for CFOs

This scorecard helps you assess your organization's cyber readiness and identify areas for improvement. For each category, select the box that best describes your current status.

Readiness Area	Key CFO Action	✅ Completed	🟡 In Progress	❌ Not Started
Governance	Cybersecurity discussed at every Audit Committee meeting.	☐	☐	☐
Incident Response	Cyber tabletop exercise run with leadership in the past 12 months.	☐	☐	☐
Patch Management	Company-wide patching policies enforced and audited.	☐	☐	☐
Insurance Alignment	Cyber insurance reviewed annually and aligned with risk tolerance.	☐	☐	☐
AI Usage Governance	Documented and communicated internal GenAI use policies.	☐	☐	☐
Internal Risk Committee	Cross-functional risk group (Finance, Legal, HR, CISO) meets quarterly.	☐	☐	☐
Vendor and Cloud Risk	Third-party vendors assessed for cybersecurity and insurance.	☐	☐	☐
Voice + Wire Fraud Protection	Safe words and verification protocols for sensitive requests.	☐	☐	☐
Security Stack Optimization	Regular audit of security tools to avoid overlap and reduce attack surface.	☐	☐	☐
Workforce Awareness	Regular employee training on phishing, AI risks, and insider threats.	☐	☐	☐

How Did You Score?

- **8–10 Completed:** 🏆 *Cyber-Confident CFO!* You're taking the right steps—keep tightening governance.
- **5–7 Completed:** ⚠️ *At Risk.* Prioritize plugging key gaps within the next 90 days.
- **0–4 Completed:** 🚨 *Vulnerable.* It's time to escalate cybersecurity to a strategic priority ASAP.

Next Steps

- Prioritize "Not Started" areas first.
- Schedule a cyber tabletop exercise with leadership.
- Review your insurance and patching policies this quarter.