The Five Named Mark Lynd Frameworks For 2026

A Working Operating Model For AI And Cybersecurity Governance Across Public Sector, SLED, Commercial, And Enterprise Organizations

Mark Lynd

5x CIO/CISO · Top 5 Globally Ranked In AI And Cybersecurity (Thinkers360, #1 Cybersecurity 2023)
Head Of Executive Advisory And Strategy · Netsync
marklynd.com

Contents

1. The 72-Hour IR Executive Playbook

RANSOMWARE RESPONSE

The 72-Hour IR Executive Playbook is the executive layer above the SOC. Built from more than 150 executive tabletop exercises across SLED, commercial, and enterprise organizations, the framework maps every hour of the first three days to the executive decision that has to land in that hour.

Phase 1, The First 6 Hours

Goal. Collapse parallel narratives into one war room with one incident commander, one source of truth, and one regulator clock. Five decisions land in this phase. Declare the incident formally with a written timestamp. Name the executive incident commander, rarely the CISO. Lock the communication perimeter. Freeze press, customer, and regulator messaging. Set a literal clock counting up from incident declaration.

Phase 2, Hours 6 Through 24

Goal. The company starts spending money. Outside counsel, forensics retainer activation, ransom posture decision, customer notification posture, and the first regulator notification draft. The pattern that breaks here is when the company has not pre-decided the ransom posture. The board update template at hour 12, hour 24, and hour 48 has six fields. What we know, what we do not know, what we are doing about it, what could change in the next 12 hours, what we need from the board, and what the next update will cover.

Phase 3, Hours 24 Through 72

Goal. The press calls. Restoration begins. The CEO is the highest risk speaker in the first 72 hours. Press protocol holds the CEO inside the war room until communications agrees on the external statement. Restoration runs daily 30 minute reviews with the CFO in the room because by hour 48 you are usually three to seven days from a recovery cost estimate that will surprise the board.

2. The Cyber Insurance Readiness Score

CYBER INSURANCE

Carriers score you. The Cyber Insurance Readiness Score lets the policyholder side score itself first, see what the carrier is going to see, and walk into renewal already knowing the number it will be assigned. Five dimensions, weighted the way carriers actually weight them.

> **Dimension 1. Identity Posture.** Privileged access, MFA coverage, conditional access, and how quickly a leaver loses access. Single fastest premium lever.

> **Dimension 2. Detection And Response.** EDR coverage, SOC hours, mean time to detect and contain, and whether the IR retainer is signed before something happens.

> **Dimension 3. Backup And Recovery.** Immutable backups, time from detonation to recovery, the date of the last full restore test, and whether the recovery plan has been run end to end with the CFO in the room.

> **Dimension 4. Vendor And Supply Chain.** Third party risk, software bill of materials maturity, and what happens to the business if the third largest vendor goes down for a week.

> **Dimension 5. Executive Readiness.** Tabletop exercise frequency, the existence of a 72-Hour IR Executive Playbook on file, the named ransom posture, and the named breach communications protocol. Invisible at quote time. Devastating at claim time.

3. The Enterprise AI Trust Score

AI GOVERNANCE

Boards have started asking the AI question. The Enterprise AI Trust Score scores an organization on five dimensions weighted the way regulators, auditors, and boards are starting to weight them. Output is a single number between 0 and 100 plus a per dimension breakdown.

> **Dimension 1. Data Lineage.** Where the training data came from, what license terms apply, what personal information is in it. Maps directly to HIPAA, EU AI Act, and discovery requests.

> **Dimension 2. Model Provenance.** Which models, who built them, what they have been benchmarked on, and whether you can pull a copy of the exact weights you are running today.

> **Dimension 3. Output Governance.** What the model is allowed to do and say, what gets logged, and what triggers human review.

> **Dimension 4. Identity And Access For AI Agents.** Agent identity, authorization, audit, and rollback. The dimension nobody had to think about a year ago and now everyone has to.

> **Dimension 5. Adversarial Resilience.** What happens when somebody tries to break your AI on purpose. Prompt injection, model poisoning, adversarial inputs.

4. The AI Board Briefing Triangle

BOARDS

Boards work in threes because three is what fits on a page and what people remember. The AI Board Briefing Triangle structures every quarterly board AI update around three corners on a single page with one decision attached.

> **Corner 1. Strategic Bets.** What is AI supposed to deliver. Three to five named bets, each with an owner, a budget, and a measurable outcome.

> **Corner 2. Risk Surface.** What does the AI deployment expose the organization to. Fed by the Enterprise AI Trust Score. Above 80, green. Below 60, red. Between 60 and 80 names the lowest dimension and the cost to close it.

> **Corner 3. Adoption Velocity.** How fast is AI moving across the organization. Counted by teams running production AI plus teams running shadow AI, plotted quarter over quarter. The dangerous pattern is high Adoption Velocity with low Trust Score.

5. The AI Adoption Tipping Point Model

AI STRATEGY

There is a moment in every AI deployment where the system crosses a line. Before, AI is helpful and optional. After, AI is load bearing. If it goes down, something in the business goes down with it. Most enterprises miss the moment because there is no announcement. The model maps four stages with a named threshold between each.

> **Stage 1. Experiment.** Small, optional, observable. Two engineers and a Slack channel.

> **Stage 2. Pilot.** Constrained deployment with named users, named outcomes, and named exit criteria. Threshold to next stage. AI moves from defined user list to default tool.

> **Stage 3. Embedded.** AI is part of how work gets done. Process disruption follows any outage. Threshold to next stage. AI outage stops being inconvenient and starts being expensive.

> **Stage 4. Load Bearing.** The business breaks if the AI breaks. Revenue declines, customers complain, SLAs miss. Triggers mandatory adoption of the Enterprise AI Trust Score, the AI Board Briefing Triangle, and the 72-Hour IR Executive Playbook as full operating model.

6. How The Frameworks Connect

The five frameworks are designed to interoperate. The Enterprise AI Trust Score feeds the Risk Surface corner of the AI Board Briefing Triangle. The 72-Hour IR Executive Playbook covers the executive layer when an incident reaches the AI Adoption Tipping Point Model load-bearing stage. The Cyber Insurance Readiness Score covers the financial dimension that a breach surfaces. Together they form a working operating model for AI and cybersecurity governance across public sector, SLED, commercial, and enterprise organizations.

Mark Lynd is a five-time CIO and CISO, Top 5 globally ranked thought leader in both AI and cybersecurity (Thinkers360, ranked #1 cybersecurity in 2023), and Head of Executive Advisory and Strategy at Netsync.