Cyber Incident "Run of Show" - Board oversight from Day 0–90

1. Before a Breach (T-minus: steady state)

Board (oversight and approvals)

- ☐ Approves incident response (IR) and business continuity (BCP) plans.
- ☐ Approves data map and geo-regulator inventory (e.g., SEC, GDPR, NIS2, UK, APAC, ME).
- ☐ Approves cyber insurance strategy and breach vendor panel (counsel, IR, forensics, PR).

Management (execution)

- ☐ Maintains IR/BCP playbooks and runs regular tabletop exercises.
- ☐ Keeps data/geo map, regulator notification matrix, and contact lists current.
- ☐ Validates backups, recovery objectives, and business continuity workarounds.
- ☐ Applies the same incident-response playbook to major third-party of supply-chain incidents where vendor breach materially affects systems, data or ability to operate

Counsel / Breach coach

- ☐ Pre-negotiates MSAs and privilege structures for incident response.
- ☐ Develops regulatory decision trees and disclosure templates across key regimes.

Insurer / Vendors

- ☐ Confirms panel terms, SLAs, and onboarding for rapid activation in a breach.

Board "pre-incident" questions

- ☐ When was our last full-scale cyber tabletop, and what changed as a result?
- ☐ Can you show us the current data/geo regulator map and notification matrix?
- ☐ Are breach counsel and key vendors engaged, conflict-free, and contractually ready to go?

2. Day 0–4: Discovery, Triage, Materiality Setup

Day 0–1 (first 24–48 hours)

Management

- ☐ Detects incident, activates IR plan/war room, preserves logs and evidence.
- ☐ Notifies CISO, CIO, GC, CEO, and triggers relevant playbooks.

Counsel / Breach coach

- ☐ Is formally retained and stands up a privileged investigative framework.
- ☐ Retains forensics and incident-response vendors.
- ☐ Insider Trading blackout once a potentially material incident is identified and NDAs for briefed insiders.

Insurer

- ☐ Is notified per policy; confirms panel providers and coverage conditions. [Ransomware negotiations]
- ☐ Confirms whether cyber-extortion (ransomware) coverage is in force and outlines required claims steps

Board

- ☐ Chair or designated committee is notified within 24–48 hours of any potentially material incident.
- ☐ Receives a short, factual briefing: what happened, so-what, now-what.

Day 2–4 (containment, scoping, early regulatory clock)

Management

- ☐ Refines scope, continues containment/eradication, activates BCP workarounds.

Forensics / IR

- ☐ Establishes initial fact base: vector, affected systems, exfiltration indicators, business impact.
- ☐ Confirms whether the incident involved encryption, data exfiltration, or both and whether extortion demands are present.

Counsel / Breach coach

- ☐ Maps facts to regulatory timelines: SEC Form 8-K, GDPR, NIS2, UK and sector rules.
- ☐ Drafts initial regulator and market disclosures as needed.
- ☐ For ransomware/extortion, assesses legality) e.g., sanctions risk), options (restore from backups versus negotiate), and coordinates with insurer-provided negotiators where appropriate.

Insurer (if ransomware/extortion)

- ☐ Confirms ransom-related coverage, conditions, and use of approved negotiators
- ☐ Coordinates with counsel and management on any engagement with threat actors

Board

- ☐ Reviews management's materiality framework and recommendation ("likely material," "borderline," "non-material but reportable").
- ☐ Confirms the company is determining materiality "without unreasonable delay" and understands that the SEC 4-business-day clock starts at materiality determination, not discovery.

- ☐ For ransomware/extortion, receives a summary of options (pay/do not pay/partial), legal and regulatory constraints, and expected precedent/ethical implications before any recommendation is finalized.

Board questions in the first 4 days

- ☐ What do we know, what is still uncertain, and how often will you update us?
- ☐ How are you determining materiality, and which regulatory clocks are already running for us?
- ☐ Is the investigation structured under privilege and aligned with our disclosure obligations?
- ☐ If this is ransomware or extortion, what are our lawful options, what alternative to payment exist, and how are insurer and negotiators being used?

3. Day 5–30: Notifications, Stabilization, Early Lessons

Day 5–14 (notification and stabilization)

Management

- ☐ Executes customer, partner, and employee notifications as required by law or contract.
- ☐ Stabilizes production and coordinates with major clients, suppliers, and other stakeholders.

Counsel / Breach coach

- ☐ Files or oversees regulatory notices (DPAs, NIS2 authorities/CSIRTs, ICO/NCSC, sector regulators) and any required SEC Form 8-K.
- ☐ Aligns messaging across regulators, customers, markets, and media.

Insurer / Vendors

- ☐ Deliver forensics, restoration, call-center, monitoring, PR, and, where applicable, ransom-negotiation support under policy.

Board

- ☐ Receives a deeper briefing: timeline, scope, regulatory posture, expected financial exposure, and communications plan.
- ☐ Confirms disclosures are accurate, consistent, and avoid premature, overly definitive statements.

Day 15–30 (recovery and early lessons)

Management

- ☐ Completes core recovery, decommissions backdoors, and hardens the environment.
- ☐ Begins structured root-cause analysis and lessons-learned process.

Forensics

- ☐ Delivers interim and then final reports under privilege on cause, scope, and control failures.
- ☐ Counsel / Breach coach
- ☐ Coordinates follow-up with regulators, investor relations, and plaintiffs' counsel, including supplemental disclosures where needed.

Counsel/Breach Coach

- ☐ Coordinates follow-up with regulators, investor relations, and plaintiffs' counsel, including supplemental disclosures where needed.

Board

- ☐ Reviews interim root-cause and remediation roadmap (spend, milestones, timeline).
- ☐ Validates that regulatory, contractual, and policy-driven duties are met or on track.

Board questions in Days 5–30

- ☐ What are the main drivers of financial, operational, and reputational impact?
- ☐ How are regulatory notices coordinated with market and customer communications?
- ☐ What lessons have already been translated into concrete changes?

4. Day 31–90: Remediation, Disclosures, Governance Uplift

Management

- ☐ Delivers and executes the remediation program (technology, process, third-party, human factors).
- ☐ Updates policies, standards, and training to embed lessons.

Counsel / Breach coach

- ☐ Supports post-incident regulator interactions, consent orders, and undertakings.
- ☐ Helps refresh SEC, EU, UK, and other risk-factor and governance disclosures.

Board

- ☐ Incorporates lessons into committee charters, board education, and cyber oversight cadence.
- ☐ Oversees refreshed disclosures and medium-term cyber risk posture.

Board questions in Days 31–90

- ☐ How are we tracking remediation to completion, and what metrics will we see?
- ☐ How are we updating public risk-factor disclosures and governance descriptions?
- ☐ What should change in our committee charters and board education plan?

Board Responsibilities for a Cyber Breach

LEGEND: R – Responsible (executes) **A** – Accountable (ultimate decision) **C** – Consulted **I** – Informed

Activity	Board / Committee	CEO	CISO / CIO	GC / External Breach Counsel	Insurer	IR / Forensics / BCP Vendors
Maintain cyber strategy, risk appetite, IR/BCP oversight	**A**	R	C	C	I	I
Maintain data/geo regulator map and notification matrix	**I**	A	R	C	I	C
Approve vendor and counsel panel (incl. breach coach)	**A**	R	C	C	C	C
Activate incident response plan on discovery	**I**	A	R	C	C	R
Engage external counsel under privilege	**I**	C	I	A/R	I	I
Notify insurer and activate panel vendors	**I**	A	C	C	R	R
Forensic investigation and technical scoping	**I**	C	C	C	C	R
Materiality assessment (SEC and analogous regimes)	**C/A** (oversight, not mechanics)	A	C	R	I	I
Decision/content of regulatory filings (SEC, DPAs, NIS2…)	**C/A** (oversight, tone at the top)	A	C	R	I	I
Customer / partner / employee notifications	**I**	A	C	C	C	R
Market / investor comms and risk-factor updates	**A** (oversight of tone and completeness)	R	C	C	I	I
Remediation roadmap approval and funding	**A**	R	C	C	I	C
Post-incident review, governance and charter updates	**A/R**	C	C	C	I	I
Ransom/extortion strategy and decision	**C/A** (oversight, risk appetite, precedent)	A	C	R	C (*)	C

* **Insurer** – Coverage, negotiators and sanctions checks

Cristina Dolan – dolan@alum.mit.edu