Board Cybersecurity Handbook

A director-level handbook for governing cyber risk, challenging management and overseeing resilience without becoming the security operations team.

GOVERN	CHALLENGE	ASSURE	PREPARE	LEARN
Risk appetite	Management	Controls	Crisis	Outcomes

BOARD PURPOSE

Give directors a practical language and operating model for cybersecurity oversight: what the board should know, what it should ask, which evidence matters and when cyber risk requires a strategic decision.

YAKAMICHI PERSPECTIVE

The board does not need to run cybersecurity. It must ensure cybersecurity is being run with sufficient competence, evidence and resilience for the enterprise's risk.

Contents & Director's Guide

SECTION	CONTENT
01	The Board Cybersecurity Mandate
02	Cyber Risk Appetite & Materiality
03	Understanding the Enterprise Attack Surface
04	Identity, Data, Cloud & Critical Technology
05	Cyber Resilience, Recovery & Business Continuity
06	Third-Party & Supply-Chain Cyber Risk
07	Cyber Metrics, Assurance & Investment
08	Cyber Incident & Crisis Oversight
09	Board Reporting, Questions & Governance Rhythm
10	180-Day Board Cybersecurity Program
A–F	Dashboard, Questions, Incident Card, Investment Test, Annual Calendar & Checklist

What Directors Should Do

- Set expectations for cyber risk appetite, resilience and management accountability.
- Challenge whether material risks are understood and funded.
- Ask for evidence that critical controls and recovery capabilities work.
- Ensure major incidents have clear escalation, disclosure and crisis governance.
- Review lessons from incidents, exercises and assurance findings.

BOUNDARY

Board oversight is not operational command. Directors should govern outcomes, risk, accountability and evidence while management retains responsibility for security operations.

The Board Cybersecurity Mandate

Cybersecurity is an enterprise risk because digital dependence connects technology failure to revenue, operations, customers, regulation, safety, reputation and strategic execution.

BOARD RESPONSIBILITY	PRACTICAL OVERSIGHT
Risk governance	Understand material cyber exposures and risk appetite
Management accountability	Know who owns cybersecurity and critical-service resilience
Strategy	Consider cyber dependencies in transformation, M&A and major investments
Resources	Assess whether management has credible capability and funding
Assurance	Require independent evidence for consequential controls
Crisis readiness	Understand escalation, decision rights and board role during incidents

Board Competence

- Maintain sufficient collective cyber literacy to ask informed questions.
- Use external expertise when risk or complexity exceeds board experience.
- Avoid allowing one 'cyber director' to become the sole owner of oversight.
- Include cyber considerations in strategy and risk discussions rather than isolating them in one annual presentation.

DIRECTOR PRINCIPLE

The board's role is to know whether management's cyber assumptions are credible, whether material exposure is within appetite and whether the enterprise can recover when controls fail.

Cyber Risk Appetite & Materiality

A useful cyber risk appetite translates broad statements into tolerances that management can design and operate against.

AREA	BOARD-LEVEL TOLERANCE EXAMPLE
Critical service outage	Maximum acceptable disruption for priority services
Sensitive data	Categories and scale of exposure requiring escalation
Identity / privilege	Tolerance for unmanaged privileged access
Recovery	Required restoration capability for critical services
Third party	Concentration or assurance conditions requiring executive action
Residual risk	Threshold above which acceptance requires executive/board visibility

Materiality Questions

- Could the event materially interrupt critical operations?
- Could it affect a significant population of customers, employees or partners?
- Could legal, regulatory or contractual obligations be triggered?
- Could the event materially affect financial position or strategic execution?
- Could uncertainty itself require escalation because consequence may be high?

APPETITE PRINCIPLE

Risk appetite should influence architecture, recovery targets, supplier decisions and investment. If it changes nothing operationally, it is only a statement.

Understanding the Enterprise Attack Surface

Boards do not need an asset-by-asset technical inventory, but they should understand where enterprise value depends on digital systems and where concentration creates disproportionate exposure.

EXPOSURE	BOARD QUESTION
Internet-facing systems	Are material externally exposed assets known and governed?
Identity	What happens if the primary identity environment is compromised?
Legacy technology	Which unsupported or difficult-to-recover systems support critical services?
Remote access	How is privileged and third-party remote access controlled?
Cloud / SaaS	Where are critical services concentrated in providers or regions?
M&A / subsidiaries	How quickly are acquired or decentralized environments brought under governance?

Board-Level Threat View

- Which threat scenarios are most relevant to our business model?
- Which systems or dependencies would create the largest enterprise consequence if compromised?
- Where does management lack visibility?
- Which material risks are being accepted because remediation is difficult or expensive?
- How does the threat environment change our investment priorities?

ATTACK-SURFACE PRINCIPLE

A board-level attack-surface view is a map of enterprise consequence, not a list of IP addresses.

Identity, Data, Cloud & Critical Technology

CONTROL PLANE	BOARD ASSURANCE QUESTION
Identity	Are privileged access and identity recovery independently protected and tested?
Data	Are critical and sensitive data identified, protected and recoverable?
Cloud	Are shared-responsibility assumptions understood and material concentration managed?
Endpoints	Can compromised devices be detected and isolated at scale?
Network	Can the organization limit lateral movement and segment critical environments?
Security tooling	Would loss of one security platform materially impair detection or recovery?

Evidence Directors Can Request

- Trend in unmanaged privileged access and remediation.
- Coverage of strong authentication for high-risk identities.
- Results of critical data recovery tests.
- Material cloud concentration and outage contingencies.
- Independent testing of critical controls and unresolved findings.

CONTROL PRINCIPLE

Ask whether the control works under realistic conditions, not merely whether a policy says the control exists.

Cyber Resilience, Recovery & Business Continuity

Boards should assume that some attacks will bypass preventive controls. Resilience oversight asks whether the enterprise can contain disruption, continue critical services and restore trusted operations.

RESILIENCE AREA	BOARD EVIDENCE
Critical services	Prioritized services with approved disruption tolerances
Dependencies	Technology, identity, data, people and suppliers mapped
Backups	Protected copies and successful restoration evidence
Recovery	Actual recovery times compared with business tolerances
Continuity	Workarounds and minimum viable operations
Exercises	Executive and technical exercises with findings tracked to closure

Board Questions After a Recovery Test

- What actually recovered and what failed?
- How long did restoration take versus approved tolerance?
- Which hidden dependency slowed recovery?
- Could recovery work if identity, cloud or communications were also unavailable?
- Which findings remain open and who owns them?

RESILIENCE PRINCIPLE

A recovery plan is an assertion. A successful recovery test is evidence.

Third-Party & Supply-Chain Cyber Risk

A critical supplier can create enterprise cyber consequence without appearing among the organization's largest vendors. Board oversight should focus on criticality, concentration and resilience.

AREA	BOARD QUESTION
Criticality	Which providers could materially interrupt a critical service?
Access	Which suppliers hold privileged or sensitive access?
Concentration	Do multiple services rely on the same provider, cloud or software dependency?
Assurance	What evidence supports confidence in critical suppliers?
Incidents	How quickly must suppliers notify and coordinate?
Exit	Can critical data/services be transitioned if the provider fails?

Board-Level Supplier Metrics

- Critical suppliers without current assurance.
- Material concentration risks above appetite.
- Critical providers without tested exit/continuity plans.
- Overdue supplier remediation.
- Material supplier incidents and notification performance.

SUPPLY-CHAIN PRINCIPLE

Diversifying vendor names does not create resilience if those vendors share the same underlying platform or geography.

Cyber Metrics, Assurance & Investment

Cyber dashboards should help directors judge exposure, capability and trajectory. Activity metrics can be useful operationally but may obscure whether enterprise risk is actually changing.

METRIC	BOARD VALUE
Critical risks outside appetite	Shows decisions and unresolved exposure
Critical control coverage	Shows whether essential protections reach material assets
Recovery within tolerance	Measures operational resilience
Material findings overdue	Shows execution discipline
Privileged access exposure	Tracks a high-consequence control plane
Critical supplier assurance	Shows external dependency coverage
Material incidents / near misses	Connects controls to real outcomes

Investment Test

- Which material risk does the investment reduce?
- What measurable capability changes after implementation?
- Is the investment addressing root cause or accumulating another tool?
- What people/process dependencies determine whether technology delivers value?
- How will management demonstrate effectiveness after funding?

METRIC PRINCIPLE

A mature dashboard contains fewer vanity numbers and more evidence tied to critical services, risk appetite and management decisions.

Cyber Incident & Crisis Oversight

During a major incident the board should avoid becoming a second incident-response team. Its role is oversight of material consequences, management decisions, disclosure governance, strategic trade-offs and stakeholder obligations.

PHASE	BOARD FOCUS
Detection / triage	Is management appropriately engaged and consequence understood?
Containment	What business impact follows from technical isolation decisions?
Investigation	What is known, unknown and how confident is management?
Disclosure / communication	Are legal, regulatory and stakeholder processes coordinated?
Recovery	What conditions must be met for safe restoration?
After action	What failed, what worked and what changes now?

Questions During a Material Incident

- What do we know, what do we assess and what remains unknown?
- Which critical services are affected or at risk?
- What major decisions has management made and why?
- What disclosure, regulatory, contractual or customer obligations are being evaluated?
- What would cause the situation to become materially worse?
- What is the recovery strategy and confidence level?

CRISIS PRINCIPLE

Boards add value by maintaining governance under pressure, not by competing with technical responders for operational control.

Board Reporting, Questions & Governance Rhythm

CADENCE	BOARD CONTENT
Each meeting	Material changes, risks outside appetite, incidents, decisions and remediation
Quarterly	Critical control/resilience trends, supplier exposure and investment progress
Semiannual	Threat scenarios, strategic dependencies and deep-dive topic
Annual	Risk appetite, cyber strategy, maturity, budget, exercise and independent assurance
Event-driven	Material incident, major acquisition, regulatory shift or significant control failure

Ten Questions Directors Should Reuse

- What changed materially since our last meeting?
- Which cyber risks are outside appetite?
- What are we least confident about?
- Which critical service would be hardest to recover?
- What evidence shows our most important controls work?
- Where are we concentrated in one provider or technology?
- Which material finding is taking too long to close?
- What cyber assumption underpins a major strategic initiative?
- What did the last exercise or incident teach us?
- What decision do you need from the board?

REPORTING PRINCIPLE

A good board cyber report ends with decisions, not merely data.

180-Day Board Cybersecurity Program

WINDOW	BOARD PRIORITY	OUTPUT
0–30 Days	Mandate & baseline	Oversight charter, accountable executives, top material risks
31–60 Days	Risk appetite	Critical-service tolerances, residual-risk escalation thresholds
61–90 Days	Evidence	Dashboard, critical-control assurance and recovery-test results
91–120 Days	Third parties & strategy	Concentration review, M&A/transformation cyber dependencies
121–150 Days	Exercise	Board/executive cyber crisis tabletop and decision review
151–180 Days	Institutionalize	Annual calendar, assurance plan, investment priorities and remediation oversight

Day-180 Board Position

- Directors can explain the organization's material cyber exposures.
- Cyber risk appetite influences management decisions.
- Critical-service recovery has evidence behind it.
- The board sees material third-party concentration.
- Cyber metrics connect to risk and resilience.
- The board has practiced its role during a severe cyber crisis.

PROGRAM PRINCIPLE

The goal is not to make directors cybersecurity specialists. It is to make cyber oversight an ordinary, evidence-based part of enterprise governance.

APPENDIX A

Board Cybersecurity Dashboard

INDICATOR	CURRENT	TREND	APPETITE / ACTION
Material risks outside appetite	__	↑ / → / ↓	Decision required
Critical services recovered within tolerance	__%	↑ / → / ↓	Target __%
Critical control coverage	__%	↑ / → / ↓	Target __%
Overdue material findings	__	↑ / → / ↓	Escalate > __
Unmanaged privileged exposure	__	↑ / → / ↓	Target __
Critical supplier assurance coverage	__%	↑ / → / ↓	Target __%
Material incidents this period	__	↑ / → / ↓	Review
Cyber investment milestones on track	__%	↑ / → / ↓	Target __%

APPENDIX B

Board Cybersecurity Question Bank

STRATEGY

- Where does digital dependency create strategic concentration?
- How does cyber risk affect our major transformation or acquisition assumptions?

RISK

- Which risks exceed appetite?
- What residual risk has management consciously accepted?

RESILIENCE

- What have we restored recently under test?
- What common dependency could defeat multiple recovery plans?

ASSURANCE

- Which critical controls have independent evidence?
- Which material findings remain unresolved and why?

CRISIS

- When would the board be notified?
- What decisions might directors need to make during a material incident?

Material Cyber Incident Board Card

FIELD	BOARD UPDATE
Situation	What happened / when detected
Business impact	Critical services, customers, data, people
Known vs assessed	Facts, judgments, confidence and gaps
Containment	Actions taken and consequence
Legal / disclosure	Processes underway; decision timing
Recovery	Strategy, dependencies and estimated confidence
Decisions	Management / board decisions required
Next update	Time / trigger

INCIDENT CARD

Keep updates decision-centered. Technical detail should be included when it changes consequence, confidence, legal obligations or recovery.

APPENDIX D

Cyber Investment Challenge Template

QUESTION	MANAGEMENT RESPONSE
Material risk addressed	_____
Current exposure / evidence	_____
Proposed capability	_____
Expected risk reduction	_____
People/process dependencies	_____
Alternative options considered	_____
Success measure	_____
Post-investment assurance date	_____

APPENDIX E

Annual Board Cybersecurity Calendar

PERIOD	FOCUS
Q1	Risk appetite, top risks, annual strategy and investment plan
Q2	Critical-service resilience, recovery testing and third-party concentration
Q3	Threat outlook, strategic transformation/M&A and control assurance
Q4	Executive exercise, maturity review, next-year priorities and assurance plan
Event-driven	Material incidents, major regulatory changes or significant control failures

APPENDIX F

Board Cybersecurity Maturity Model & Checklist

LEVEL	CHARACTERISTICS	BOARD MEANING
1 — Reactive	Incident-led updates; technical metrics; unclear appetite	Limited governance visibility
2 — Developing	Regular reporting, top risks and initial resilience evidence	Oversight improving but uneven
3 — Managed	Risk appetite, assurance, recovery evidence and crisis exercises	Repeatable board governance
4 — Adaptive	Cyber integrated with strategy, capital, suppliers and continuous learning	Cyber informs enterprise choices

Director Checklist

- ☐ Cyber oversight responsibilities are explicit
- ☐ Material cyber risks and accountable owners are visible
- ☐ Risk appetite includes operational tolerances
- ☐ Critical-service recovery is tested
- ☐ Critical control assurance is reported
- ☐ Third-party concentration is understood
- ☐ Metrics connect to risk and resilience
- ☐ Board crisis role has been exercised
- ☐ Material findings are tracked to closure
- ☐ Cyber considerations are integrated into strategy and major investments

Yakamichi Perspective

Strong board cyber governance creates productive tension: management is empowered to operate, while directors insist on clarity about material exposure, credible evidence and the enterprise's ability to recover.

REQUEST A CONFIDENTIAL CONSULTATION

United States: +1 202 413 3763 | Maryland, USA
Nigeria: +234 811 095 0651 | Abuja, Nigeria

YAKAMICHI • Artificial Intelligence • Cybersecurity • Counter-Surveillance • Corporate Risk Intelligence