Communicating Cybersecurity to Stakeholders

- Turn cyber risk into stakeholder decisions, not technical reports
- Boards and regulators now expect quantified risk, clear accountability, oversight evidence
- Roadmap: stakeholder mapping, business language, board reporting, incident communication
- Key terms: stakeholder, risk appetite, materiality, cyber resilience, decision-ready reporting
- 2026 standard: financial exposure, trend direction, and a clear decision point



The 2026 Communication Bar:
What Stakeholders Now Expect

- Cyber is a standing board agenda item, with deep dives at least quarterly
- Oversight structures, reporting lines, and cadence now appear in public filings
- Common failures: jargon, activity metrics, good-news-only reporting, no follow-up
- A CISO may get 5–10 minutes; select the vital few messages
- If only good news is reported, the board is blind to systemic weaknesses



Know Your Audience: Stakeholder Map and Information Needs



- Six stakeholder segments, six different core concerns
- Board: direction and risk appetite; C-suite: financial and operational impact
- Business units: continuity and delivery; regulators and auditors: evidence and method
- Customers: trust and action; employees: practical guidance
- Map decision rights: who approves budget, accepts risk, or blocks progress
- Match format to persona: risk-return for CFO, recovery time for operations
- Avoid mismatches: vulnerability counts to boards, vague updates to engineers

From Technical Findings to Business Language



Technical Finding
CVE and host
(technical detail)

Risk to Decision

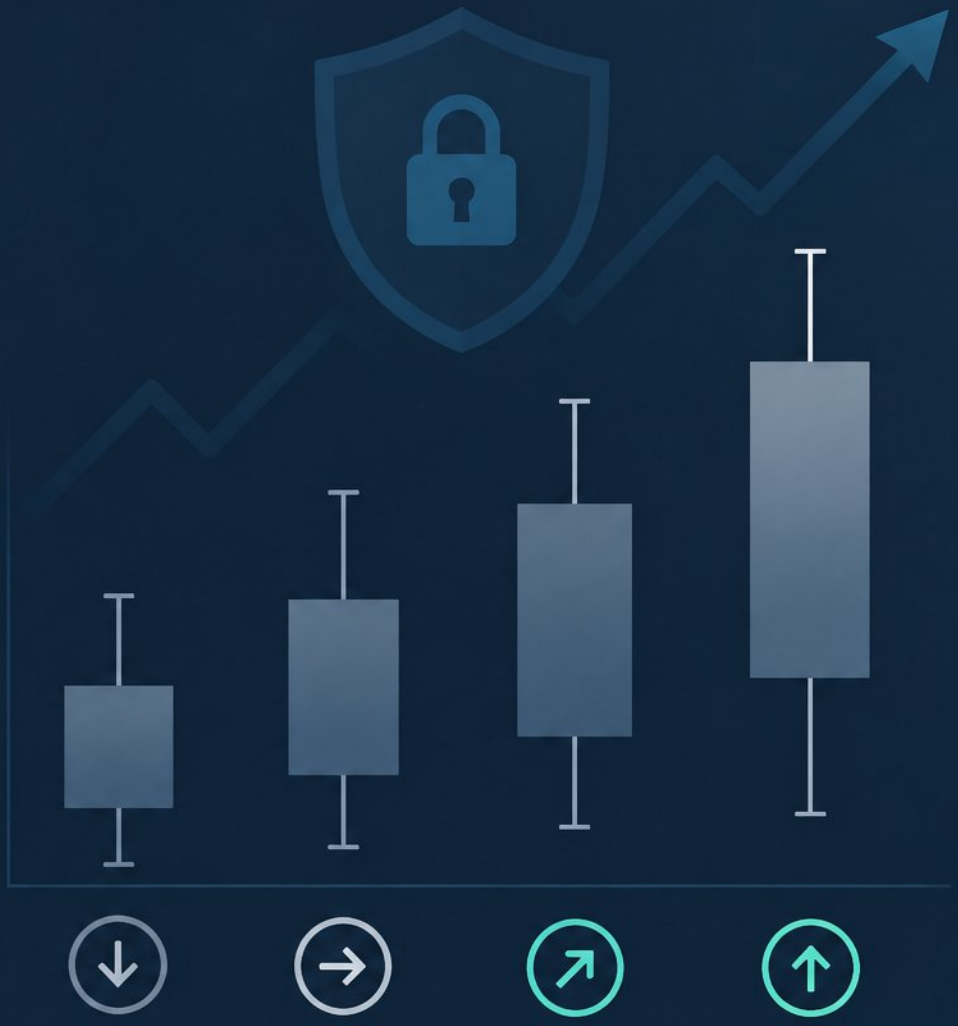


Business View
Dollar exposure,
trend, and cost to close
(business context)

1. **Match abstraction to audience:** engineers need CVE and host; executives need dollar exposure, trend, and cost to close
2. **Frame impact by business category:** revenue interruption, customer churn, regulatory exposure, downtime, recovery time
3. **Use plain, jargon-free language;** explain at an absurdly high level, then add detail only if asked
4. **Keep one consistent model across briefings** so infrequent audiences engage quickly and compare periods
5. **Avoid fear-based or speculative messaging:** state credible likelihood and impact with explicit assumptions and confidence

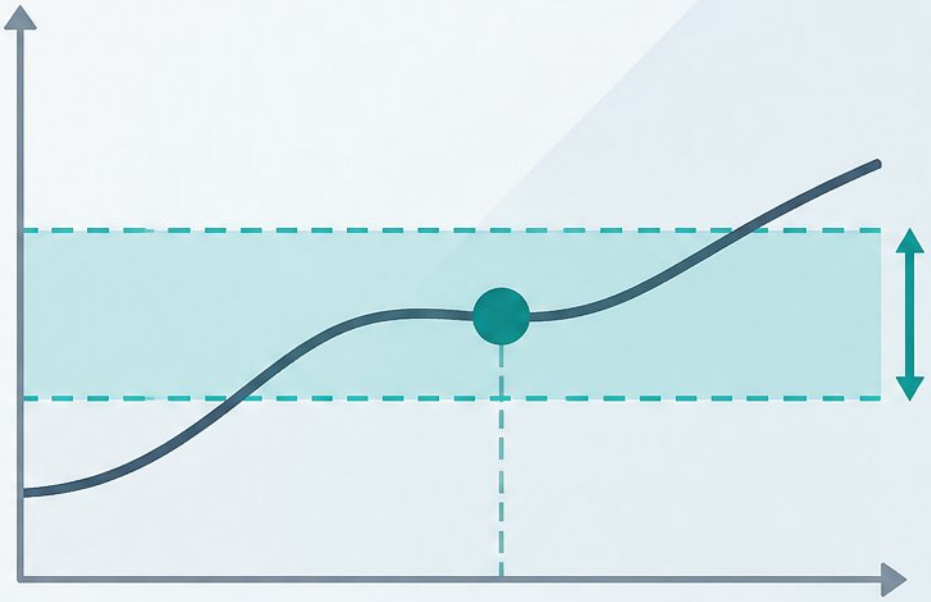
Quantifying Cyber Risk in Financial Terms

- Heat maps orient discussion but obscure real exposure differences
- FAIR produces annualized loss ranges and scenario-based probable financial impact
- FAIR use or planned adoption reached 58% in 2026, up from 46% in 2025
- Report the vital few loss scenarios, not one aggregate exposure figure
- Every board metric needs a dollar value, trend direction, and decision point



Framing Risk Against Appetite, Materiality, and KRIs

- Risk appetite statements tell stakeholders: in tolerance, or who accepts residual risk?
- Document materiality judgment and escalation thresholds before an incident, not during
- KRIs should be ratios tied to risk variance — not activity counts like incidents worked
- Align cyber reporting with ERM language, cadence, and metrics used for other material risks
- State assumptions and uncertainty openly; withheld uncertainty reads as dishonesty



Board and Executive Reporting That Drives Decisions

- 20–30 minute board item: posture, compliance, performance, incidents, emerging risks, the ask
- Six to eight slides plus appendix; every data point tells one story
- Cyber-Risk Brief standing item: two-page memo plus dashboard
- Material-incident update: one-page sheet within 24 hours of determination
- Quarterly deep-dive workshop for strategy, threats, and budget alignment
- The ask slide: each decision or risk acceptance listed separately with rationale
- Audit committee: method and data lineage, control effectiveness in dollars, concentration risk
- Stable minimum metric set each quarter so directors see change, not new formats



Preparing for Tough Board Questions

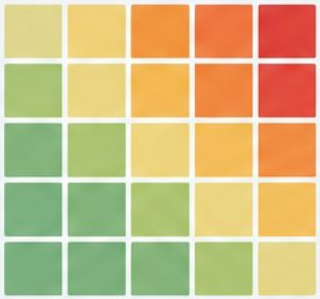
- Anticipate standard oversight questions: risk appetite, crown jewels, response testing, third-party governance
- AI exposure is a standing concern: inventory, shadow AI, data flows, human-in-the-loop, NIST AI RMF
- Separate supplier risk from dependency risk; check concentration across critical providers
- Answer "Do you have what you need?" with objective evidence, labeling judgment as judgment
- Prepare by role: board wants concise data; CFO needs materiality confidence; legal needs process discipline



Visuals and Formats for Executive Audiences

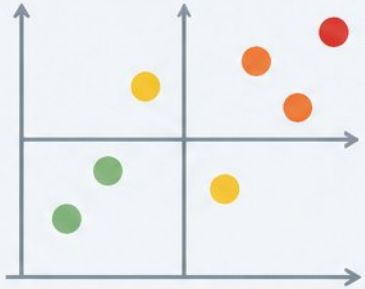
CLEAR VISUALS. BETTER DECISIONS.

Heat Map



Helps decide which risks need attention now.

Risk Quadrant



Helps decide where to focus and how to act.

Trend Line



Helps decide if risk is increasing or improving.

Traffic Lights



Helps decide what needs action now.

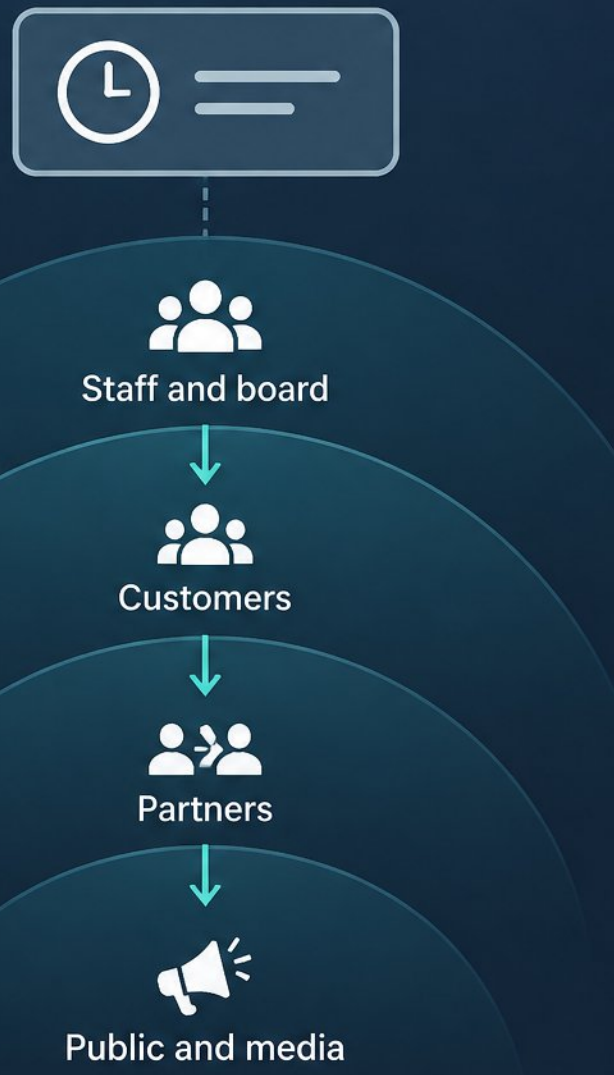
- Match each visual to the decision: heat maps, quadrants, trends, traffic lights
- Heat maps: top 10–15 risks, 5x5 grid, plain labels, one-line "so what"
- One-page summary: posture, top three risks, compliance, 4–6 health metrics
- Show trends not snapshots; label honestly; cut chart junk; test the 10-second read
- Avoid overcrowding, inconsistent colors, and red items with no action

SIMPLE FORMATS. STRONGER INSIGHTS.

Communicating During a Cyber Incident

CLEAR MESSAGES. THE RIGHT ORDER. A STRONGER RESPONSE.

- Pre-assign roles: incident lead, communications lead, trained spokesperson, legal, government relations
- Communicate inside-out: staff and board, then customers, then public and media
- One source of truth: state what is known and unknown, no speculation
- Fixed update cadence by severity, with timestamped updates even when nothing changed
- Keep messages consistent and aligned with legal and regulatory positions



Meeting Regulatory Notification and Disclosure Obligations

AWARENESS
TO ACTION
TO COMPLIANCE



Awareness or Determination

GDPR
Art. 33



Notify supervisory authority within 72 hours of awareness

NIS2
Art. 23



24-hour early warning



72-hour notification

Final report in one month

DORA



Classification-driven clocks; initial notice within 24 hours of awareness

SEC 8-K Item 1.05



File within four business days of materiality determination

- Statutory clocks start at awareness or determination, not investigation end
- GDPR Art. 33: notify supervisory authority within 72 hours of awareness
- NIS2 Art. 23: 24-hour early warning, 72-hour notification, final report in one month
- DORA: classification-driven clocks; initial notice within 24 hours of awareness
- SEC 8-K Item 1.05: file within four business days of materiality determination
- Align public statements with legal counsel and regulatory filings



After the Incident: Rebuilding Trust with Customers and the Board

LEARN
IMPROVE
MOVE FORWARD



- Manage the aftermath deliberately: acknowledge impact, commit to fixes, skip marketing language
- Customer updates should be actionable, honest about uncertainty, aligned to specific harm guidance
- Close the board loop with a factual report: timeline, impact, notifications, root cause, fixes
- Treat near-misses as learning signals; reward escalation, not silence
- Feed every lesson back into templates, playbooks, and exercise schedules

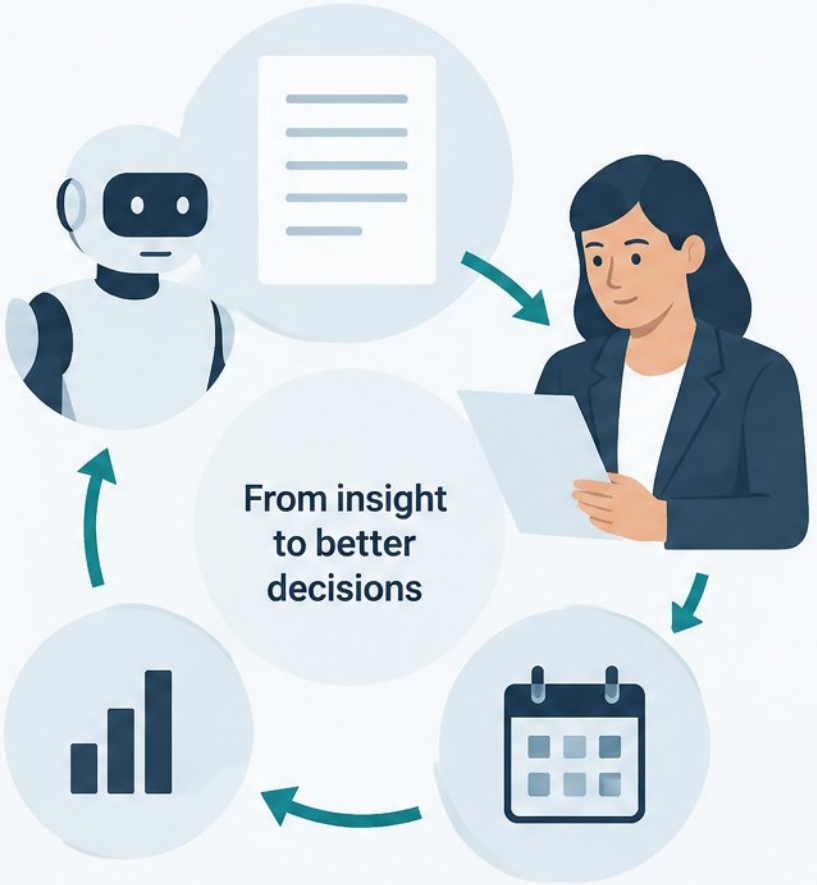
Everyday Engagement:
Turning Security into a Business Partnership

- Build a rhythm: a short board item every meeting, plus deeper quarterly sessions
- BISOs embed in business units; security champions embed in engineering teams
- Nominate champions, don't assign them: time allocation and management backing required
- One security staff member can support around five champions
- Influence without authority: frame requests around business outcomes
- Reward honest error reporting; treat security as a dialog, not a mandate



AI-Assisted Reporting and Measuring Communication Effectiveness

- AI drafts and summarizes; humans own every material claim and risk decision
- Define authoritative metric sources; separate operational facts from interpretation
- Mandate human review of board material; keep confidential data out of public tools
- Measure outcomes: decision velocity, funding won, board feedback quality, fewer stilted questions
- Close the loop after every briefing and adjust the next report
- Action plan: personal goals, stable metric set, engagement calendar for two quarters



Technical finding → **Business decision**

PersonWise.

PersonWise • AI digital-human course platform



Scan the code or click anywhere to watch this course live, with voice Q&A

personwise.ai/t/05ee3360/public