The Loss Exceedance Curve Playbook

A Field Manual for Quantitative Cyber Risk Communication

This is a tactical reference for using loss exceedance curves to make and defend security decisions. It covers eight operational use cases, each with a scenario, modeling steps, presentation guidance, and sample stakeholder language.

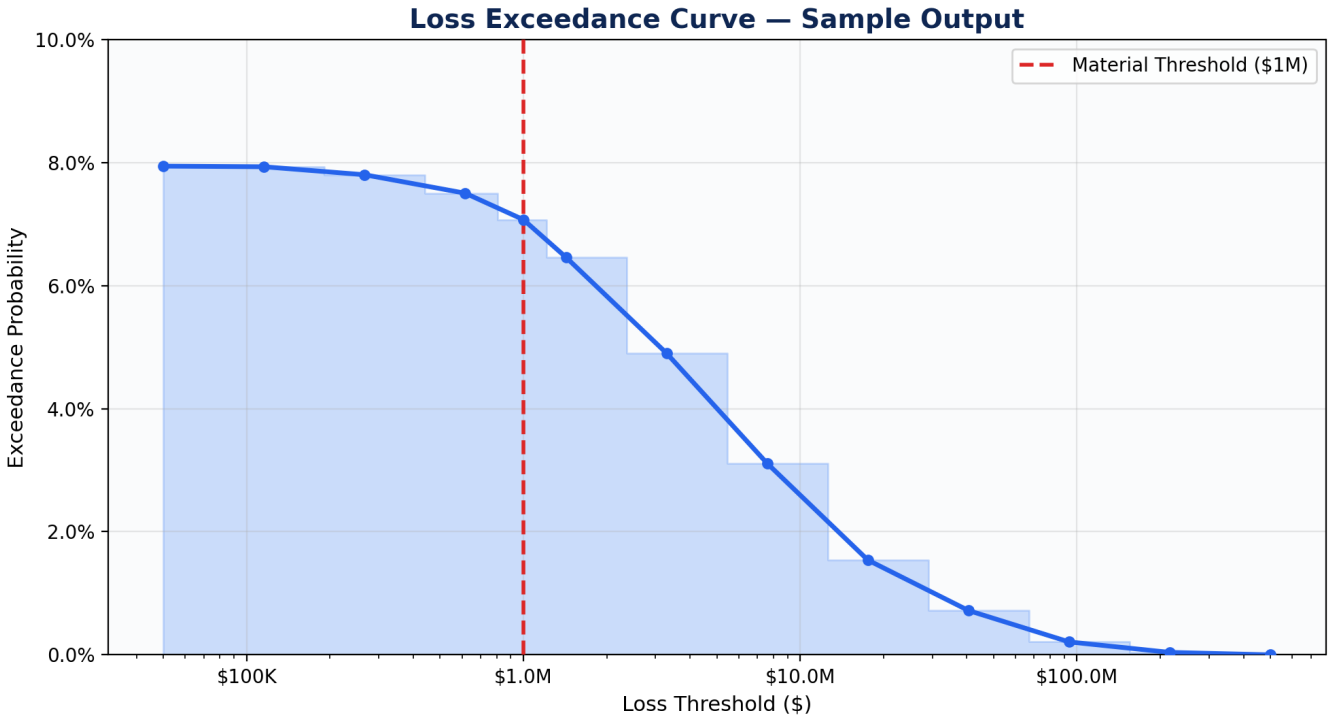
The companion LEC workbook is available at **learnfirstprinciples.com**. This document assumes familiarity with the five-variable model: outside-in probability, inside-out reduction, loss bounds (90% confidence interval), and material threshold.

Brandon Karpf | **2026**

Contents

1. The One-Page LEC Briefing

Every use case in this manual references the same underlying output: the loss exceedance curve. This page shows you how to read it.



How to read this chart: The x-axis shows loss thresholds in dollars (log scale). The y-axis shows the probability that losses exceed each threshold. The curve always slopes downward: smaller losses are more probable than larger ones. The dashed red line marks your organization's material threshold.

Metric	Value	What It Means
Combined Probability	8.0%	Annual chance of any loss event occurring
P(Loss > $1M)	7.1%	Annual chance of a material breach
Expected Annual Loss	$386K	Probability-weighted average loss per year
Median Loss (given event)	$1.5M	50th percentile if an event occurs
90th Percentile Loss	$11.7M	Worst-case-but-plausible loss scenario

2. Communicating Total Risk Exposure to the Board

> *Scenario: You are presenting to a non-technical board of directors. They need to understand the organization's cyber risk posture in financial terms.*

What to Show

Lead with the Decision Support chart that shades the full curve. The single-sentence annotation ("There is an X.X% chance of a breach in the next twelve months") gives the board an anchor before they see any detail. Follow with the material breach chart showing the probability of losses exceeding the threshold the board cares about.

Present three numbers: the combined annual probability, P(loss exceeds material threshold), and the Expected Annual Loss. These three metrics tell a complete story: how likely, how bad, and what it costs you on average per year.

What to Say

> *"Based on industry data and our internal controls assessment, our model estimates an 8% annual probability of a cyber loss event. There is a 7.1% chance that losses exceed our $1 million materiality threshold. Our expected annual loss is approximately $386,000. This represents the probability-weighted cost of cyber risk to our organization per year."*

What to Leave Out

Do not present the simulation mechanics, the lognormal distribution parameters, or the number of Monte Carlo trials. The board does not need to know how the sausage is made. If asked, explain that the model uses 10,000 simulated scenarios based on five inputs calibrated to industry data.

Handling "What's the Exact Number?"

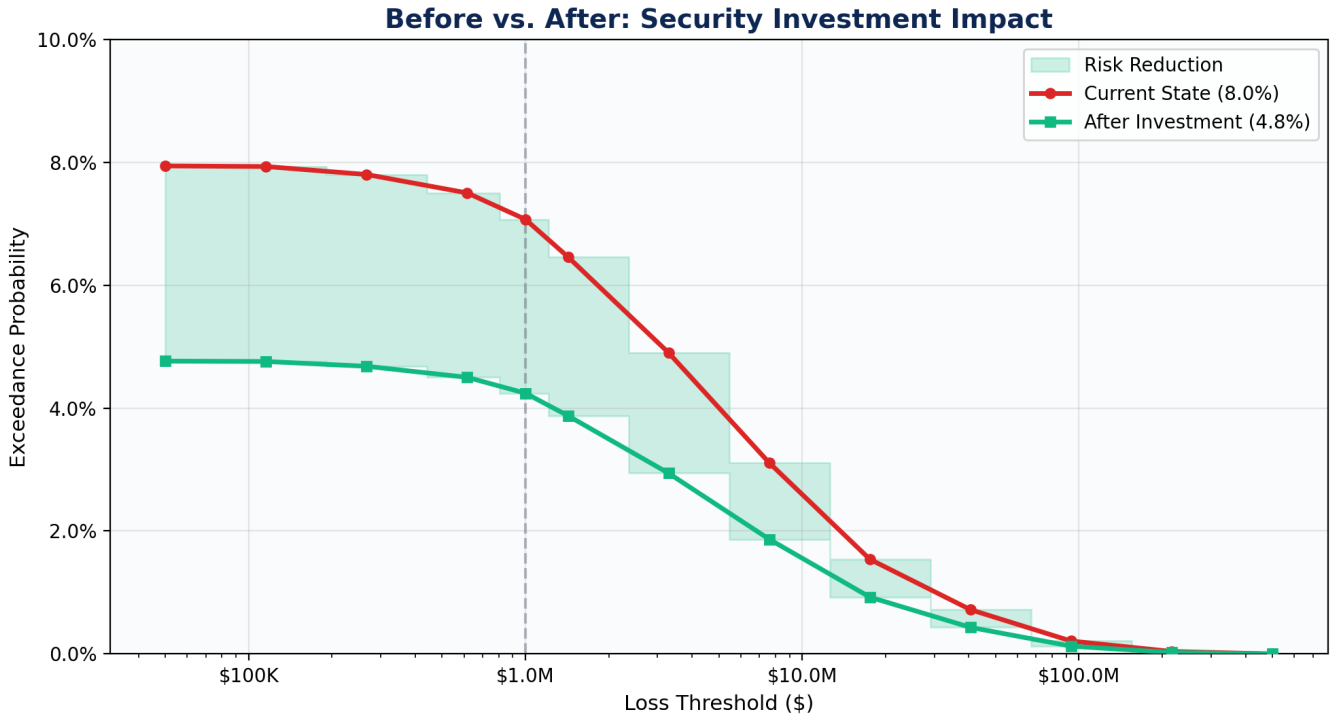
Boards sometimes want a single dollar figure. Redirect to the percentile table: "If an event occurs, there is a 50% chance losses stay below $1.5 million, but a 10% chance they exceed $11.7 million. The curve gives us the full distribution, not a single guess." This framing respects the uncertainty rather than hiding it.

Level 2: Recurring Board Reporting

Run the LEC quarterly. Save copies of the workbook with each quarter's inputs. Present the trend: "In Q1, our P(exceed $1M) was 8.2%. After deploying XDR and hiring two analysts, Q3 shows 5.1%." This transforms a static snapshot into a program performance metric that the board can track over time.

3. Evaluating Security Tool Investments

Scenario: A vendor pitches a $500K endpoint detection tool that claims to reduce breach risk. You need to determine whether the investment has a positive expected return.



How to Model It

Step 1: Run the LEC with your current inputs. Record the Expected Annual Loss (EAL). Step 2: Estimate how the tool changes your inputs. A strong EDR solution might increase your inside-out reduction by 1–3 percentage points, or it might narrow your loss bounds by reducing the upper bound (faster detection means smaller breaches). Step 3: Run the LEC again with the adjusted inputs. Record the new EAL. Step 4: Calculate the delta.

The Decision Rule

Metric	Current State	After Investment	Delta
Inside-Out Reduction	2.0%	4.0%	+2.0%
Combined Probability	8.0%	6.0%	−2.0%
Expected Annual Loss	$386,000	$231,000	−$155,000
Annual Tool Cost			$500,000
Net Annual Value			($345,000)

In this example, the tool reduces EAL by $155K/year, but costs $500K/year. The investment has a negative expected return at these assumptions. Adjust the inside-out reduction upward or narrow the loss bounds further if the vendor's claims justify it. If you cannot make the numbers work with reasonable assumptions, the tool is not worth the investment.

What to Present

Show the two curves overlaid (current state vs. post-investment). The green shaded area between the curves represents the risk reduction the tool provides. "The gap between these two curves is worth $155,000 per year in expected loss reduction. The tool costs $500,000. At these assumptions, the tool does not pay for itself. We need to find a solution that either costs less or reduces risk more."

4. Justifying Budget to the CFO

Scenario: Annual budget cycle. The CFO wants to know why security needs $2.5M next year. You need to frame the ask in financial terms the CFO responds to.

The Framing

CFOs respond to ROI, not fear. Do not lead with breach horror stories. Lead with the current expected annual loss, the projected EAL if the budget is approved, and the delta. Frame the security budget as a risk reduction investment with a quantifiable return.

How to Model It

Map each budget line item to its effect on the five LEC variables. A SOC expansion increases inside-out reduction. A vulnerability management program narrows the loss bounds by reducing the likelihood of catastrophic exploitation. An incident response retainer lowers the upper bound by accelerating containment. Run the LEC for each scenario: current state, partial budget, full budget.

Sample Language

"Our current expected annual loss from cyber events is $386,000, with a 7.1% chance of a material breach exceeding $1 million. The proposed $2.5 million security budget reduces expected annual loss to $148,000 and cuts material breach probability to 3.2%. The net risk reduction is $238,000 per year in expected value. The investment does not eliminate risk. It brings our exposure within the tolerance the board set last quarter."

Using Multiple LECs

Build a separate LEC for each major risk scenario (ransomware, data breach, insider threat). Present them as a portfolio. The CFO sees which risks drive the most expected loss and which budget line items address each one. This prevents the common failure mode where the entire security budget is justified by a single scary scenario.

5. Driving Hiring and Talent Development

Scenario: You need to justify two new security analyst headcount ($350K fully loaded) or a $200K training program for the existing team.

How to Model It

Staffing and skill gaps affect the inside-out reduction variable. An understaffed SOC with junior analysts provides less risk reduction than a fully staffed team with experienced engineers. Estimate your current inside-out reduction, then estimate what a fully staffed, well-trained team would provide. The gap between those two numbers, multiplied by the expected loss, is the cost of the staffing shortfall.

Worked Example

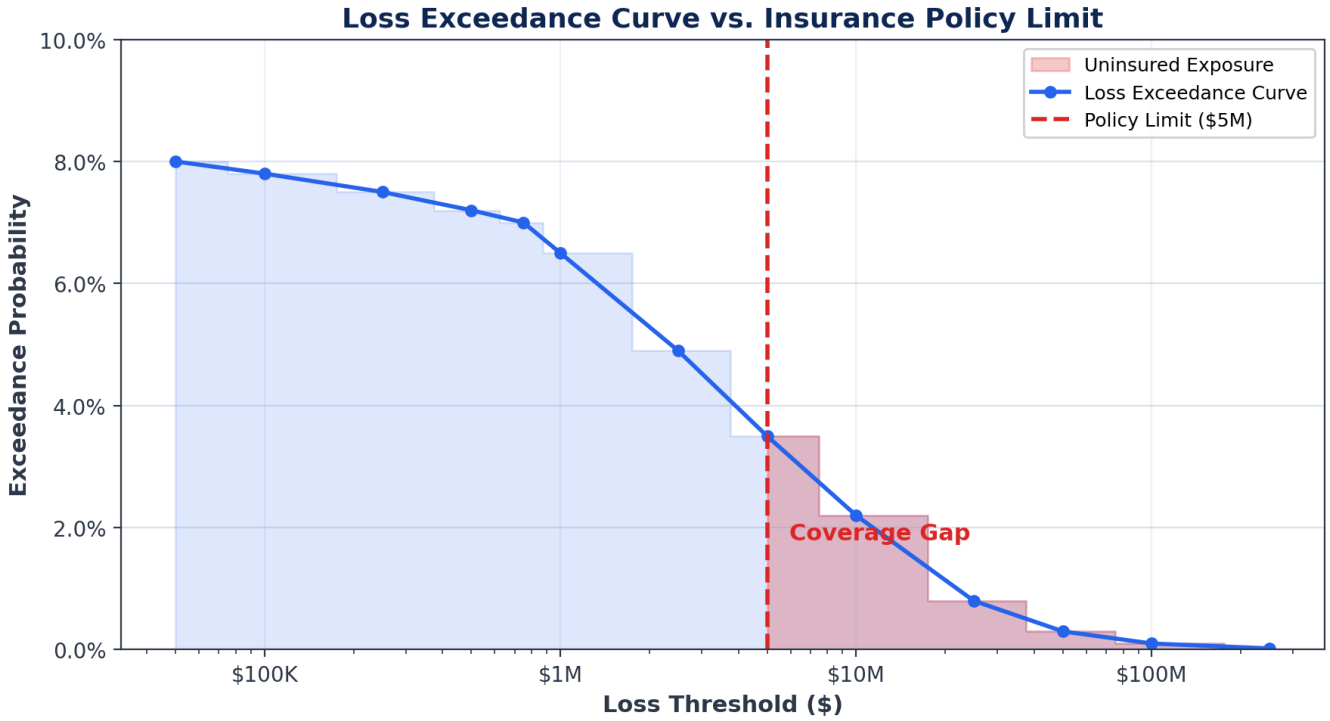
Scenario	Inside-Out	Combined Prob	EAL
Current (understaffed)	2.0%	8.0%	$386K
With 2 new analysts	3.5%	6.5%	$289K
With training program	3.0%	7.0%	$325K
Both (full investment)	4.5%	5.5%	$210K

The two analysts reduce EAL by $97K/year against a $350K cost. The training program reduces EAL by $61K/year against a $200K cost. Neither investment pays for itself in pure EAL terms within one year. The argument for hiring is not a one-year ROI calculation. It is a sustained reduction in risk posture that compounds over multiple years, combined with the operational capacity to detect and respond to incidents that the current team cannot.

Frame it accordingly: "Each unfilled analyst position represents approximately $48K in additional expected annual loss. Over three years, that is $145K per position, which exceeds the fully loaded cost of hiring."

6. Evaluating Cyber Insurance Coverage

Scenario: Your broker quotes a cyber insurance policy with a $5M limit, $250K deductible, and $180K annual premium. You need to determine whether the coverage matches your risk profile.



How to Use the LEC

The LEC percentile table tells you the distribution of losses if an event occurs. Compare those percentiles against the policy terms.

LEC Output	Value	Policy Implication
Median loss (50th %ile)	$1.5M	Covered (within $5M limit, above $250K deductible)
75th percentile	$4.2M	Covered, but approaching policy limit
90th percentile	$11.7M	Exceeds $5M limit by $6.7M (uninsured gap)
95th percentile	$18.8M	Exceeds limit by $13.8M (severe uninsured gap)

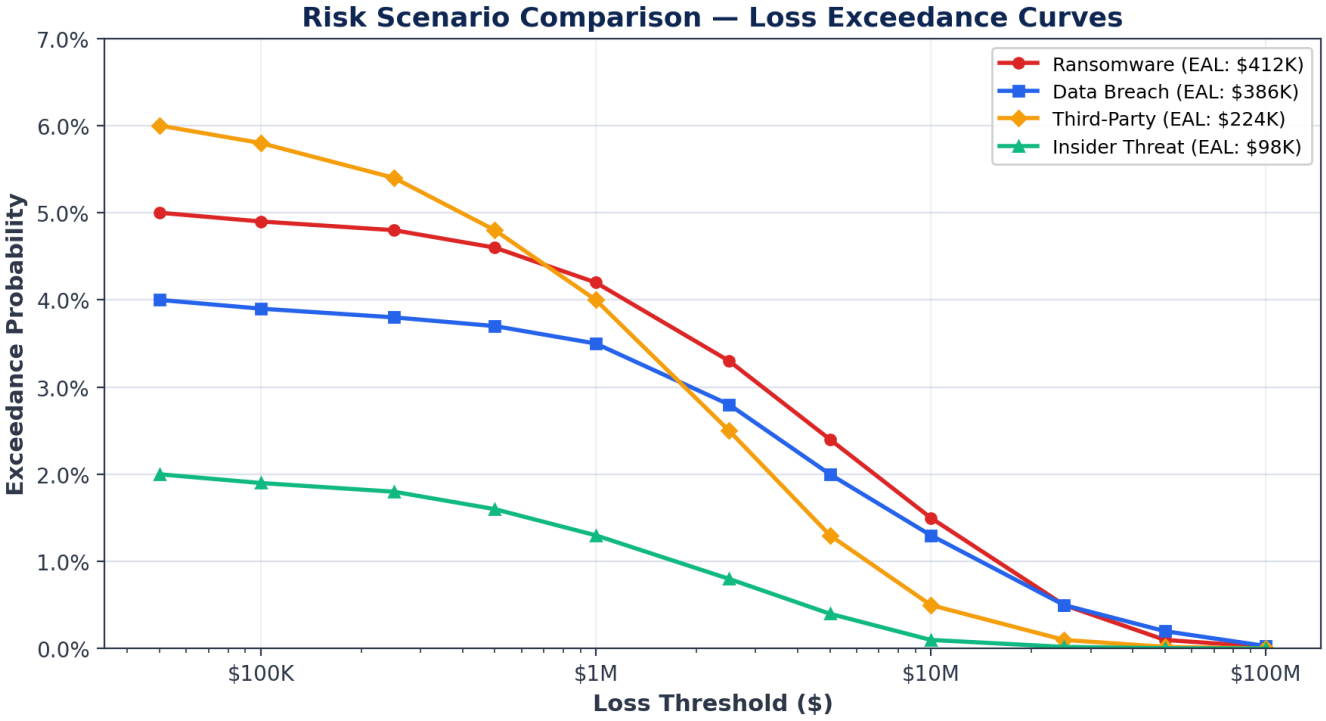
The LEC reveals that one in ten breach events would exceed the policy limit by more than $6 million. This is a quantifiable argument for requesting higher coverage limits, adding an excess policy, or increasing the deductible to reduce premium and reallocating those savings to a higher limit.

Negotiation Language

"Our loss exceedance model shows a 10% probability that breach costs exceed $11.7 million. Our current policy limit of $5 million leaves a $6.7 million gap at the 90th percentile. We need to evaluate either increasing the primary limit to $15M or adding an excess layer above $5M."

7. Prioritizing Across Risk Scenarios

Scenario: You need to allocate limited budget across ransomware defense, data breach prevention, and insider threat mitigation. Which risk gets the most investment?



How to Model It

Build a separate LEC for each risk scenario. Each scenario gets its own set of five inputs reflecting the probability and loss profile specific to that threat type. Compare the Expected Annual Loss across scenarios. The scenario with the highest EAL represents your greatest financial exposure and should receive proportional investment.

Risk Scenario	Probability	Loss Range	EAL	Priority
Ransomware	5.0%	$500K – $30M	$412K	HIGH
Data Breach (external)	4.0%	$1M – $50M	$386K	HIGH
Insider Threat	2.0%	$200K – $10M	$98K	MEDIUM
Third-Party Compromise	6.0%	$100K – $15M	$224K	HIGH

In this example, ransomware drives the highest expected annual loss despite a lower probability than third-party compromise, because the loss range is wider and the tail is heavier. Budget allocation should weight ransomware defense accordingly.

The Portfolio View

Sum the EALs across scenarios for an aggregate expected annual loss. In this example: $412K + $386K + $98K + $224K = $1.12M. This is the number to put in front of the CFO as the total cost of cyber risk. Then show how each budget line item maps to a specific scenario's EAL reduction.

8. M&A Cyber Due Diligence

Scenario: Your organization is acquiring a mid-size SaaS company. The deal team needs to quantify the cyber liability being inherited.

How to Model It

Build an LEC for the acquisition target using publicly available data and the information gathered during due diligence. Use industry breach rates for the target's sector as the outside-in probability. Assess their security maturity from questionnaire responses, SOC 2 reports, and penetration test results to estimate the inside-out reduction. Set loss bounds based on their data holdings, revenue, and regulatory exposure.

What to Present to the Deal Team

The EAL for the target becomes a quantified liability that can be factored into the deal price. "The target's expected annual cyber loss is $520,000, with a 12% probability of a breach exceeding $2 million. Over a three-year integration horizon, the cumulative expected cyber cost is $1.56 million. This should be reflected in the purchase price or addressed as a condition of close."

Post-Acquisition Tracking

After the acquisition, re-run the LEC quarterly to track how integration activities (migrating to your security stack, onboarding to your SOC, remediating identified vulnerabilities) reduce the target's risk profile. This creates an auditable record of risk reduction tied to specific integration milestones.

9. Third-Party and Vendor Risk Prioritization

Scenario: You manage 200+ vendors. Your third-party risk management program relies on questionnaires and tier ratings. You need a better way to prioritize which vendors get the most scrutiny.

How to Model It

Build a simplified LEC for each critical vendor (or vendor category). The outside-in probability comes from the vendor's industry base rate. The inside-out reduction comes from your assessment of their security controls (SOC 2 findings, questionnaire responses, external ratings). The loss bounds reflect the impact to your organization if that vendor is breached: how much of your data do they hold, what operations depend on them, what is your contractual liability.

Prioritization

Rank vendors by EAL, not by questionnaire score. A vendor with a mediocre security questionnaire but minimal access to your data may have a lower EAL than a vendor with a strong questionnaire who processes all your customer records. The LEC reveals which vendors actually represent financial risk, not just compliance risk.

Vendor	Category	Data Access	EAL to You	Action
Vendor A	Cloud EHR	All patient records	$310K	Full assessment + contract review
Vendor B	Payroll	Employee PII	$85K	Annual questionnaire
Vendor C	Marketing	Email lists only	$12K	Biennial review
Vendor D	IT Managed Services	Network access	$220K	Full assessment + pen test

This table replaces the traditional red/yellow/green vendor tier system with a financial prioritization that maps directly to assessment and remediation effort.

Quick Reference: The Five-Variable Cheat Sheet

1. Outside-In Forecast (Annual Probability)

What it is: The base rate probability of a loss event for an organization like yours, based on industry data.

Where to find it: HHS OCR Breach Portal, Verizon DBIR, Cyentia IRIS, IBM Cost of a Data Breach Report.

Common mistake: Using a generic "all industry" rate instead of sector-specific data. Healthcare and finance have 76x more breach events than the lowest-frequency industries.

2. Inside-Out Reduction

What it is: The probability reduction your security controls provide versus the industry baseline.

Where to find it: Self-assessment. Consider your SOC maturity, MFA coverage, patch cadence, detection/response capabilities.

Common mistake: Overestimating your own controls. Be honest. A 2–5% reduction is strong. Above 5% requires evidence.

3. Lower Bound (90% Confidence Interval)

What it is: The minimum plausible loss if an event occurs. You are 95% confident the loss will be above this number.

Where to find it: Incident response retainer costs, minimum notification costs, forensics floor.

Common mistake: Setting this at zero. If an event occurs, there is always a cost. Start with your IR retainer as the floor.

4. Upper Bound (90% Confidence Interval)

What it is: The maximum plausible loss if an event occurs. You are 95% confident the loss will be below this number.

Where to find it: IBM Cost of a Data Breach (industry averages), regulatory maximum fines, lost revenue modeling.

Common mistake: Anchoring to the average breach cost. The upper bound should reflect your tail risk, not the median outcome.

5. Material Threshold

What it is: The dollar amount that triggers board-level attention or regulatory reporting.

Where to find it: Ask your CFO or risk committee. This is organization-specific.

Common mistake: Picking an arbitrary round number. The threshold should reflect your organization's actual reporting and governance triggers.

The LEC workbook and all workshop tools are available free at learnfirstprinciples.com.

