EACG
Enterprise Architecture Consulting Group

SECURITY DIALOGUES
No. 2 · 14 August 2026
Marcus Hale (proponent) · Tess Calder (challenger) · Jessy Lang

Likelihood Times Impact

Why the risk matrix's arithmetic fails, and what to report instead of one number

A single number next to a finding was enough for a customer to decide to ship a patch immediately. The episode tests the five-by-five matrix: Tess wins the argument about the arithmetic, but the real objection is what the multiplication does to its inputs. One is knowable, one is a guess, and the product hides which is which.

BORROWED CERTAINTY
A guess borrows a measurement's confidence.

1. What is a three?

2. Where do the inputs come from?

3. Which half is known, which is guessed?

WHAT GOES WRONG WITH THE MATRIX AND WHAT TO DO INSTEAD

1	**A three is a word** The numeral has no unit, no zero and no defined distance to its neighbour.	You can sort with a ranking, you cannot multiply with it. Multiplying needs the step from two to three to equal the step from four to five, and nobody defined what the steps measure. Reproducible is not accurate: a broken instrument is reproducible.
2	**Same cell, different risks** Four times three and three times four both come out at twelve.	A thing that happens most quarters and costs a few days is an operating cost: budget for it and stop discussing it in the room. A thing that almost never happens and means explaining it to a regulator is a question about surviving a bad year, for different people. Do not let a multiplication put them in one cell.
3	**Borrowed certainty** The product looks as confident as the measured half and is as accurate as the guessed half.	Refuse to combine the two. Nobody downstream can tell which half was which, and a twelve does not remember where it came from. The fix is not a better formula.
4	**A proof of possible, read as probable** A penetration test shows something can happen, never that it is unlikely.	Read "high" as a ceiling, not a frequency: one authorised, motivated professional, nine days, four attempts. Neither the tester nor the risk owner is instrumented to know how often anybody tries, so the likelihood column stays a guess.
5	**The one known fact gets crushed** Impact is known: what was readable, which keys, which service accounts.	Do not compress a fact into one digit from one to five chosen by a committee that never walked the path. Multiplying it by a guess destroyed the only thing anybody actually knew.
6	**One number steers the decision** A customer shipped a patch immediately on a single number next to a finding.	Two plain sentences carried more information than the twelve, but took about four times as long, with eleven other items on the agenda and forty minutes for the whole risk portfolio. Accept that cost.

THREE PRACTICES INSTEAD OF ONE NUMBER

Two lines, not one
Known: this path was walked, here is what it reached, here is who confirmed it. Assumed: the frequency, in words, with a name attached, so that person is findable six months later.

Keep the meeting
The matrix is a table people sit at. Before it, who spoke last and loudest decided. Drop the product, keep the meeting. The price is giving up the sorted list.

Own your column
The tester does not fill in likelihood. Impact is the tester's entirely: object when it is compressed into one digit.

Listen to the episode
Likelihood Times Impact and the rest of the series.
eacg.de
/en/podcast/s02-likelihood-x-impact

Digital Product Design
From the first idea to a viable first release.
eacg.de
/en/consulting/digital-products

PSIRT Services
Intake, assess and disclose vulnerabilities, built or run as a service.
eacg.de
/en/consulting/psirt

© 2026 EACG GmbH