CYBERSECURITY FIRST PRINCIPLES

A REBOOT OF STRATEGY & TACTICS

Order the book from Amazon here.

Research on Why the Heat Maps are Poor Vehicles for Conveying Risk

2005: Surveyed NATO Officers believe that Highly Likely could mean anywhere between 40% and 100% likely.
Ronald Howard, "The Foundations of Decision Analysis Revisited."

2006: Studies find that experts choose "1" more often in a scale of say "1" to "10" regardless of the subject matter the number is supposed to represent.
Kelly See, Craig Fox, and Rottenstreich, "Between ignorance and truth."

2008: Ordinal scales inadvertently create range compression – a kind of extreme rounding error.
Louise Cox, "What's Wrong with Risk Matrices?"

2009: Surveyed students and faculty believe that "Very Likely" could mean anywhere between 43% and 99% likely.
Budescu, Broomell, and Por, "Improving Communication of Uncertainty in the Reports of Intergovernmental Panel on Climate Change."

2016: Cybersecurity scoring systems like OWASP (Open Web Access Security Project), CVSS (Common Vulnerability Scoring System), CWSS (Common Weakness Scoring System), and the CCSS (Common Configuration Scoring System) perform improper math on non-mathematical objects to aggregate a risk score.
Hubbard and Seiersen, "How to Measure Anything in Cybersecurity Risk."

2016: The idea of "Risk Tolerance" is not presented. Just because risk officers rate an event as highly likely does not mean that leadership is not willing to accept that risk.
Hubbard and Seiersen, "How to Measure Anything in Cybersecurity Risk."

2016: Heat maps convey no information about when the event might happen (e.g., next year, next three years, next decade.)
Hubbard and Seiersen, "How to Measure Anything in Cybersecurity Risk."

2016: Some risk officers rate events as more likely just because they could be more impactful.
Hubbard and Seiersen, "How to Measure Anything in Cybersecurity Risk."

2016: When percentages are explicitly defined, highly likely is between 90% and 99%; for example, survey participants violated the rules over half the time.
Hubbard and Seiersen, "How to Measure Anything in Cybersecurity Risk."

2016: Most surveyed experts using ordinal scales from "1" to "5" chose the values of "3" or "4," reducing the 5x5 matrix to a 2x2 matrix.
Hubbard and Seiersen, "How to Measure Anything in Cybersecurity Risk."