Team Meeting

How to Measure Anything in Cybersecurity Risk

Ben Goldsworthy, Brand New Consultant

Delivered 2021-11-03

Contents

Introduction

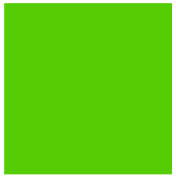
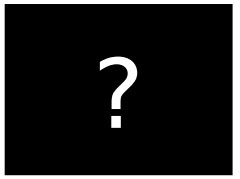
- **Lancaster University** alumnus
  - BSc. (Hons) Computer Science
  - MSc. Cyber Security
- Doing IT ‘stuff’ for **~9 years**

- **Software development** background

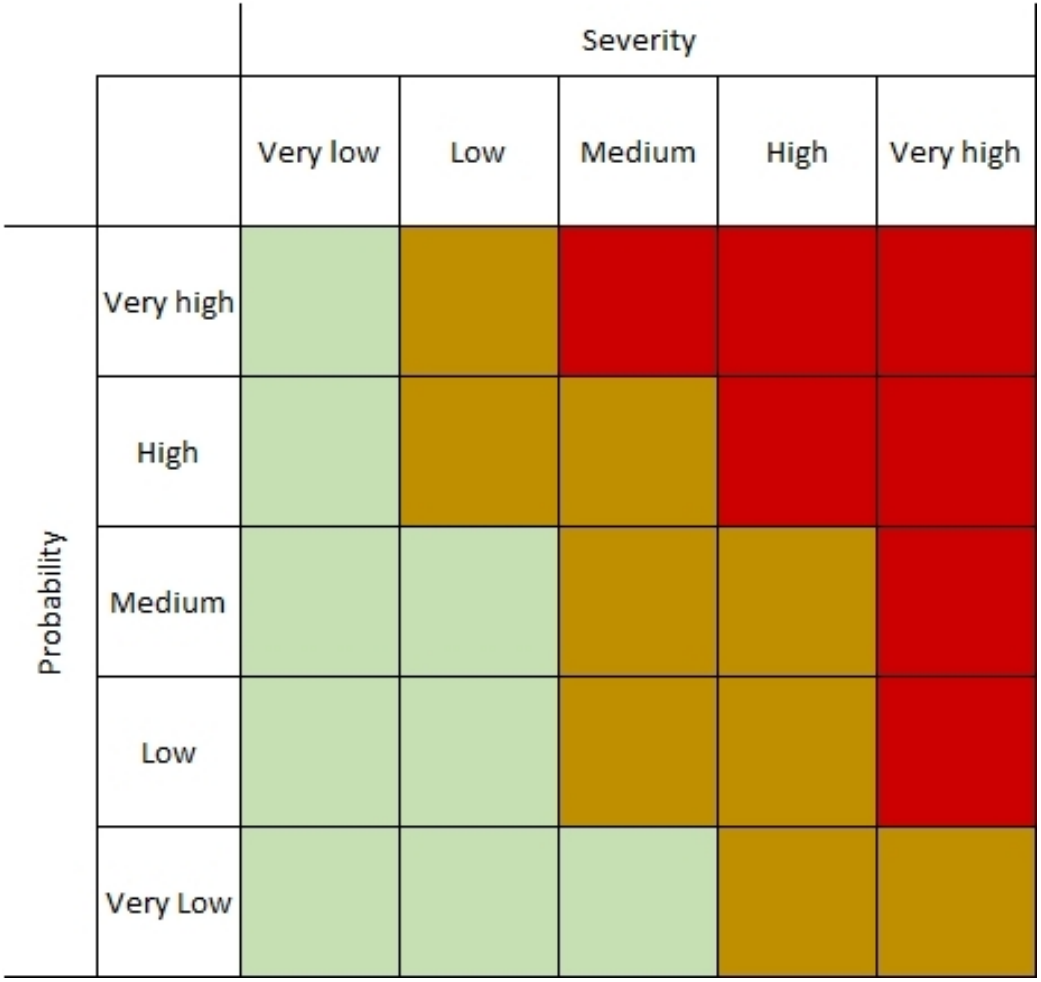
- Previously: researching **IT threat intelligence** analysis and presentation techniques, theoretically underpinned by **quantitative approaches** to risk assessment

Pop Quiz, Hotshot



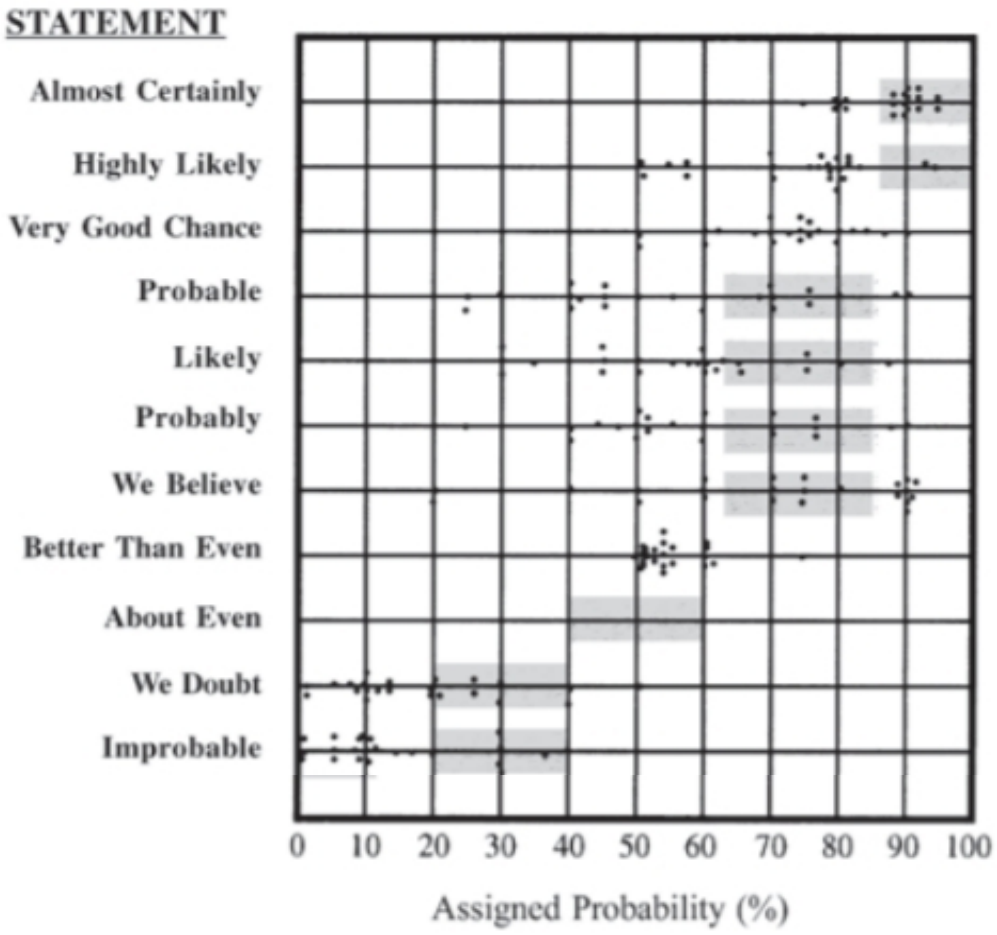




Risk Matrix



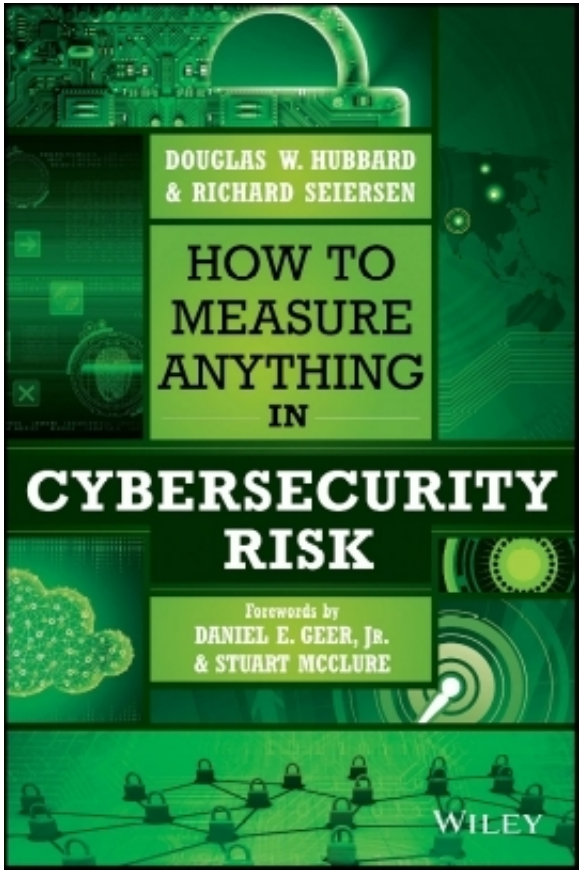
Words of Estimative Probability

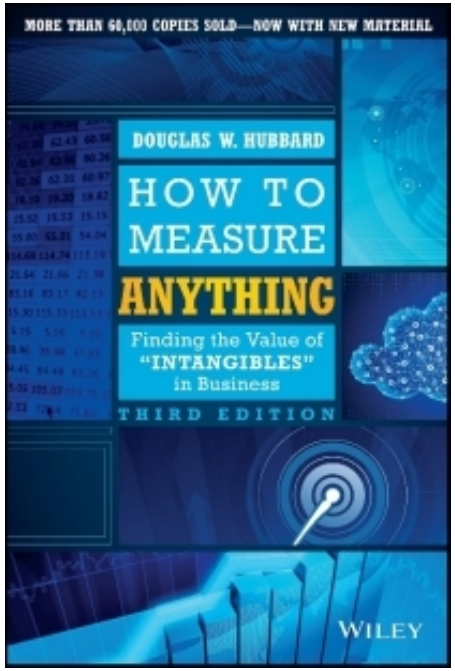
Figure 18: Measuring Perceptions of Uncertainty



Richards J. Heuer, *Psychology of Intelligence Analysts* (1999)

How to Measure Anything…





Key Assertions

- ‘There is **no evidence** that the types of scoring and risk matrix methods widely used in cybersecurity improve judgement.’
- ‘On the contrary, there is evidence these methods add noise and error to the judgement process. One researcher…goes as far as to say they can be “**worse than random**.”’
- ‘Any appearance of “working” is probably a type of “**analysis placebo**.”’
- ‘There is overwhelming evidence…that **quantitative, probabilistic methods are effective**.’

What is ‘measurement’?

Concept

Object

Methods

What is ‘measurement’?

Concept

Measurement: A quantitatively-expressed reduction of uncertainty based on one or more observations

Scales of Measurement

Concept

- **Nominal**
- **Ordinal**
- **Interval**
- **Ratio**

Interval and Ratio Scales

- **Interval:** degrees Celcius
- **Ratio:** pounds and pence

Concept

- Well-defined unit of size
- Can compare values
  - e.g., 6 is 2 more than 4
- Can’t multiply or divide intervals
  - e.g., 6 is not ‘50% more’ than 4
  - e.g., 6°C is not ‘twice as hot’ as 3°C

Nominal Scale

Concept

- No implied order or magnitude
  - e.g., gender, location
- Each state scale is just a *different* state, not a higher or lower state

Ordinal Scale

Concept

- Denote an order, but not by how much
  - e.g., privileges, 1 to 5 (counter-intuitively)

Nominal and Ordinal Scales

Concept

- Most mathematical operations are not applicable
- Still **can be** informative
- Prone to mathematical abuse

Nominal and Ordinal Scales

Concept

- ‘Geologists don’t multiply Mohs hardness scale variables times [a] rock’s color.’

Bayesian Measurement

Concept

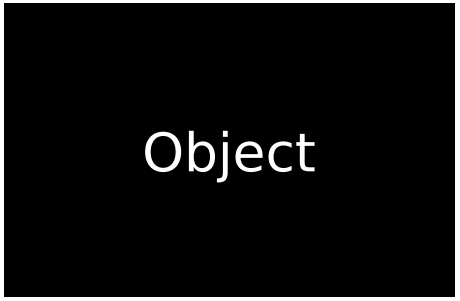
- **Probability:** the state of uncertainty of an observer (a.k.a. ‘degree of belief’)

The Object of Measurement

Object

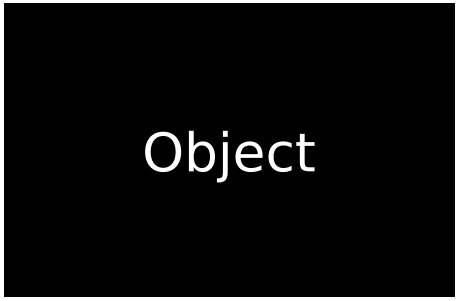
- Can you unambiguously define the **object** of measurement?
  - e.g., ‘Damage to reputation’
- What do you mean, **exactly**?

Clarification Chain



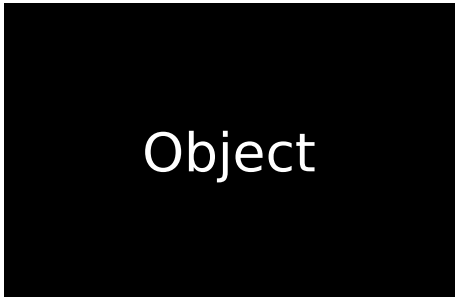
1. If it matters at all, it is detectable/observable
2. If it is detectable, it can be detected as an amount (or range of possible amounts)
3. If it can be detected as a range of possible amounts, it can be measured

Thought Experiment



- Imagine a **clone** of your organisation
- Call one the ‘test’ org., and one the ‘control’ org.
- Imagine that the ‘test’ org. has experienced a little bit more ‘**damage to reputation**’, whilst holding the amount in the ‘control’ org. constant
- What do you imagine you would actually observe?
  - Long- or short-term drop in sales?
  - Difficulty recruiting top applicants?
  - Cost of PR to offset consequences?

Risk



- **Risk:** A state of uncertainty where some of the possibilities involve a loss, catastrophe or other undesirable outcome
- **Measurement of Risk:** A set of possibilities, each with quantified possibilities and quantified losses

Risk

Methods

- ‘Cybersecurity is **not** some exceptional area **outside the domain of statistics** but rather **exactly the kind of problem** statistics was made for.’

Small Samples

Methods

- Consider a population of **1,000 different-sized widgets**
- You take a random sample of **five widgets**
- What is the chance that the **median** of the entire population (the point at which half the population is below and half above) is **between the largest and smallest** of that sample?
- **93.75%**

Rule of Five

Methods

- Chance of randomly picking a value **above the median**: 50%
- Chance of randomly selecting five values that are **all above** the median:
  -
    - Ditto for **all below** the median
- Chance of **not** getting all above/below:
  -

One-for-one Substitution

• Instead of:	• We substitute:
• Rating **likelihood** on a scale of 1 to 5	• Estimating the **probability of the event happening** in a given period of time
• Rating **impact** on a scale of 1 to 5	• Estimating a 90% confidence interval for a **monetized loss**
• Plotting likelihood and impact scores on a **risk matrix**	• Using the quantitative likelihood and impact to generate a **loss exceedance curve**
• Further dividing the risk matrix into **risk categories** and guessing what you should do	• Comparing the loss exceedance curve to a **risk tolerance curve** and prioritising actions based on return on mitigation

But wait!

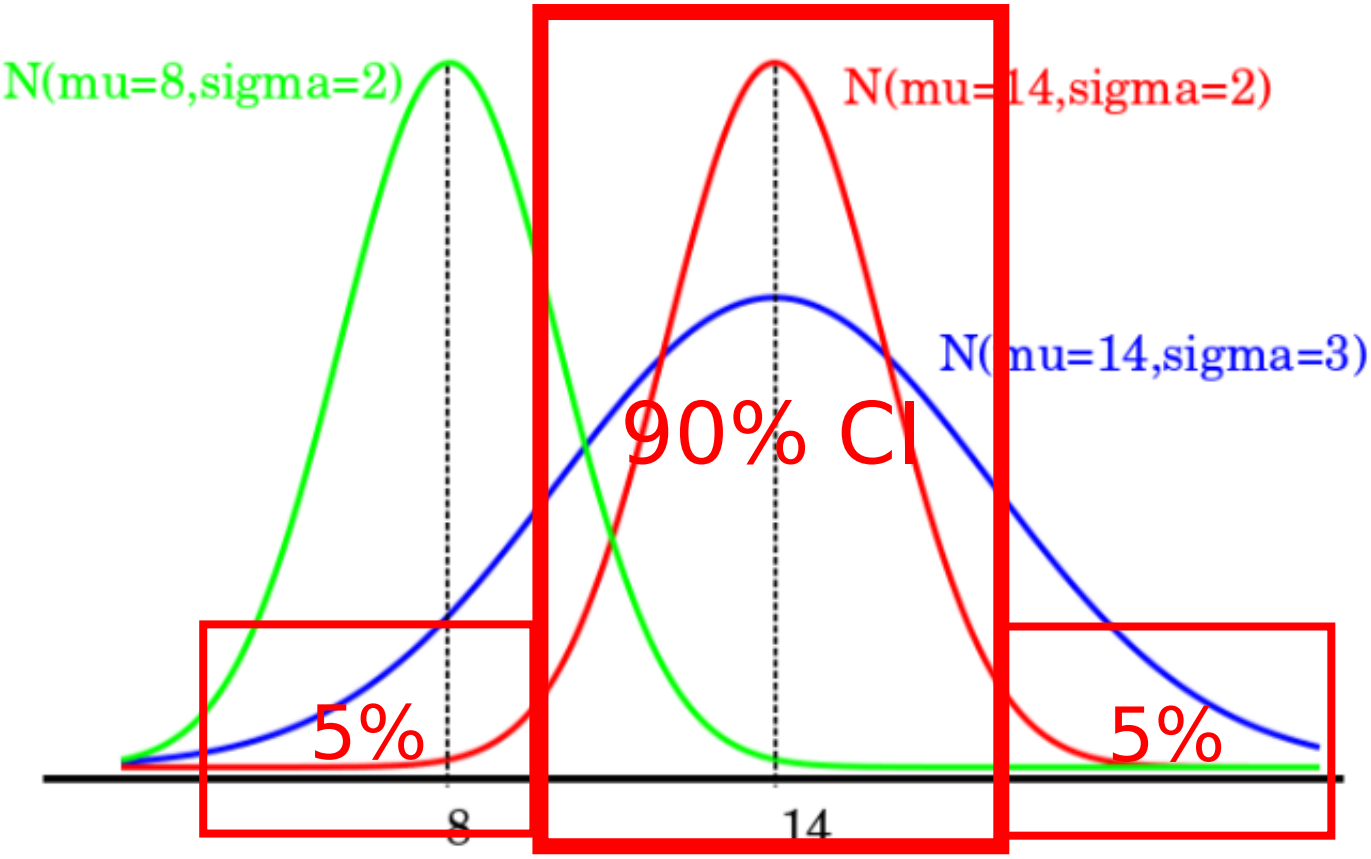
- How do we add/subtract/multiply/divide when we have no exact values, **only ranges**?

Monte Carlo Simulations

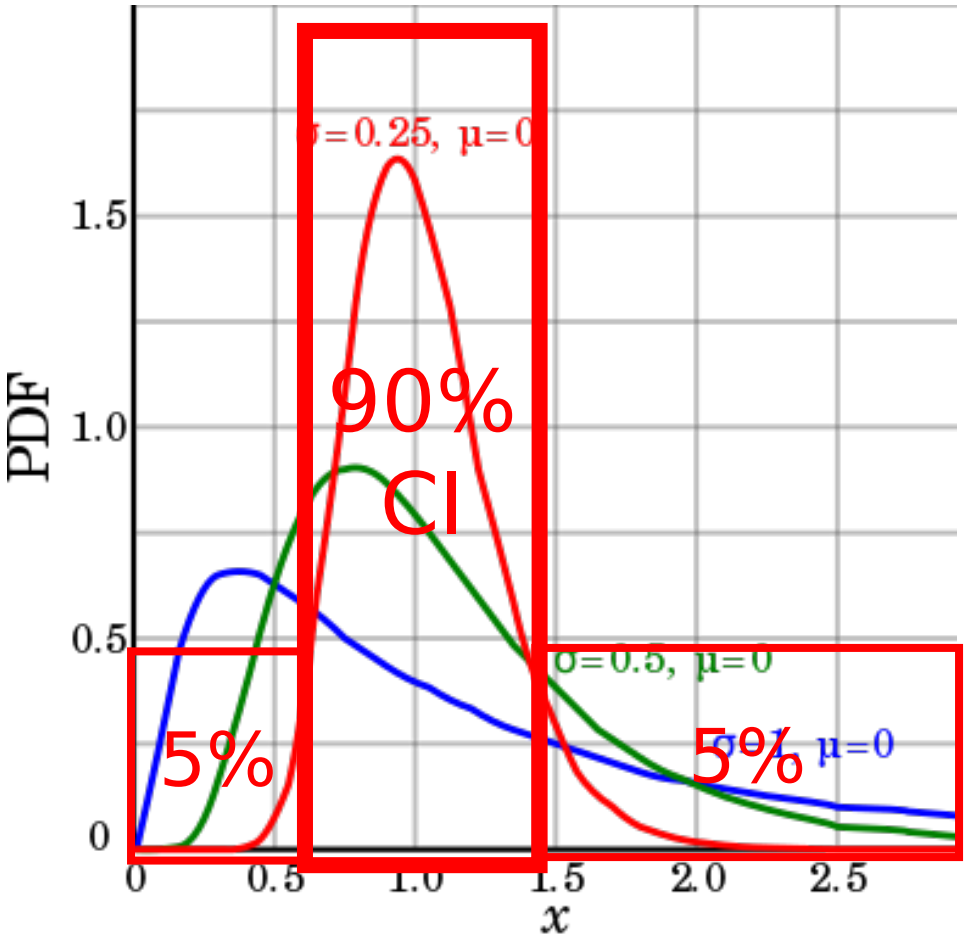
Intro. to Monte Carlo Simulations

1. Run a **large number of simulations** of your org. over a period of time (e.g., 1 year)
2. For each simulation, test whether an **event occurred** or not
3. For each simulation in which an event occurred, determine the **cost of the event**
4. Repeat steps 2 & 3 for each simulation, to taste
5. At the end of the full run of simulations, perform **what-if analyses** on the results

Normal Distribution



Log-normal Distribution

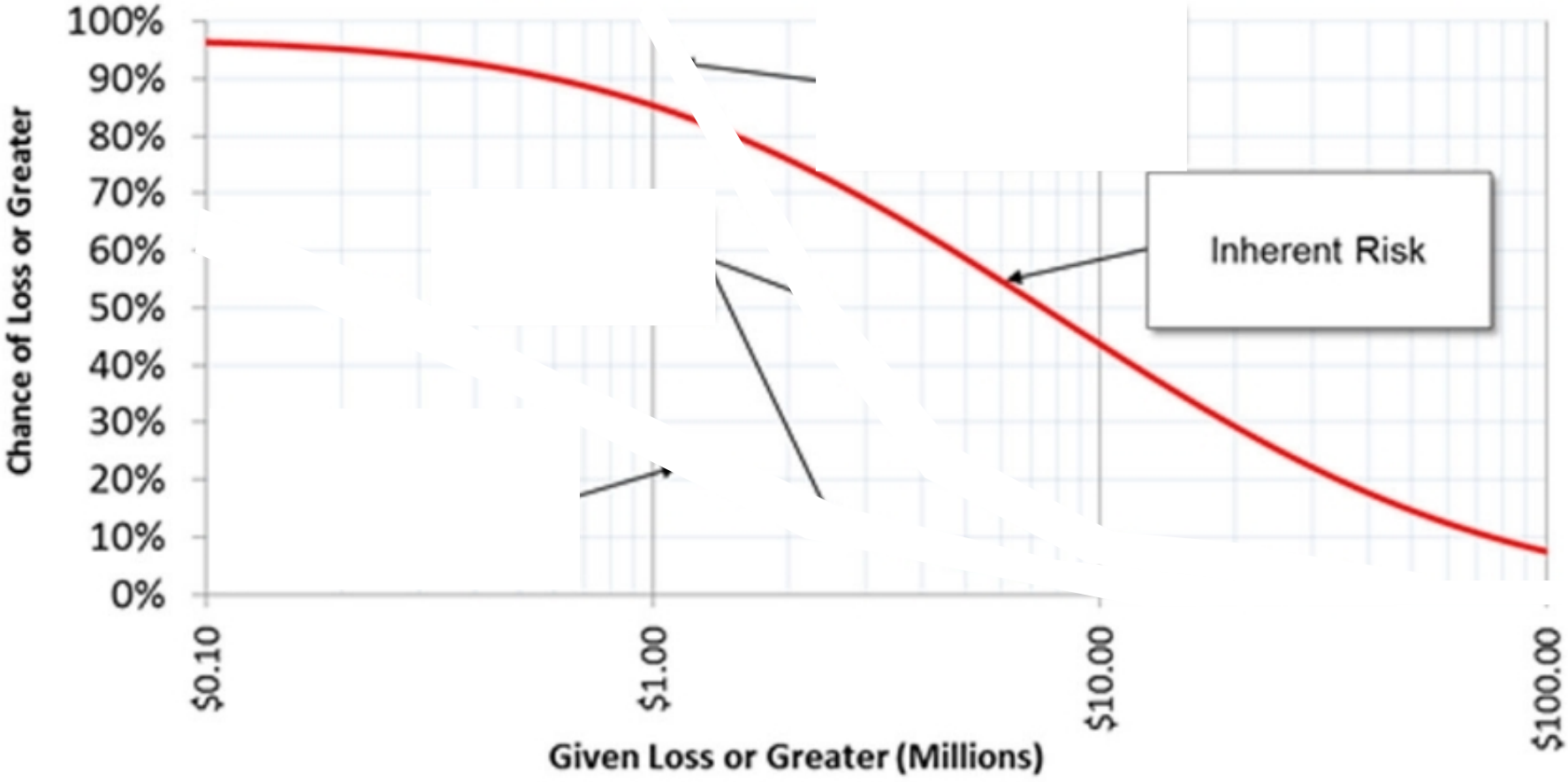


Thanks to Krishnavedala (CC0 1.0)

Example Monte Carlo Simulation

- Event has a probability of 0.15 (i.e., it happens 15% of the time)
- For each simulation run, test
- If 1, sample from a cost distribution
- Repeat as desired
- Sum the total losses for the simulation run
- Repeat for n simulation runs

Loss Exceedance Curve

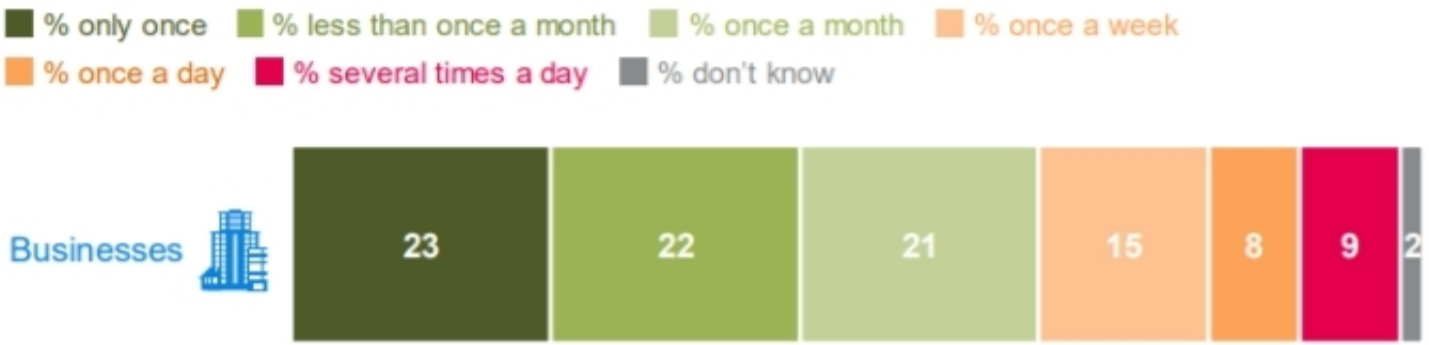


Real Example: *CSBS 2020*

Real Example
Likelihood

Figure 5.1: Percentage of organisations that have identified breaches or attacks in the last 12 months

Figure 5.4: How often organisations have experienced breaches or attacks experienced in the last 12 months



Real Example
Likelihood

-
-
-
-
- Estimated category frequency boundaries =
-
- Insert values from *CSBS:*
  -

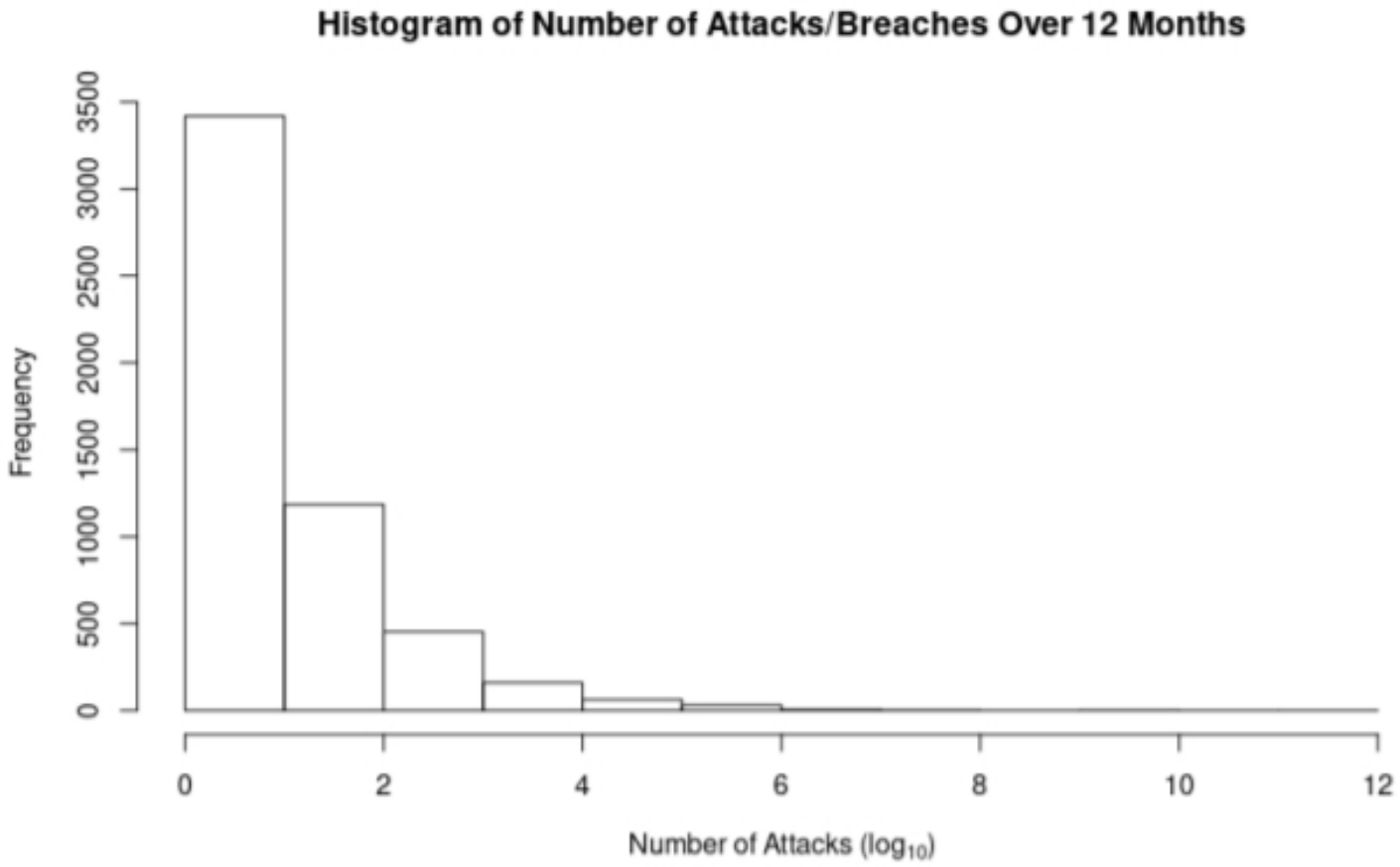
Real Example
Likelihood

- Pareto cumulative distribution function:
  -
  -
- Therefore, for :
  -
  -

Real Example
Likelihood

- Run simulations using formula (where is a uniform random number:
  -
  -
- Results from 10,000 iterations:
  -
  -
  -
  -
  -

Real Example Likelihood



Real Example
Cost

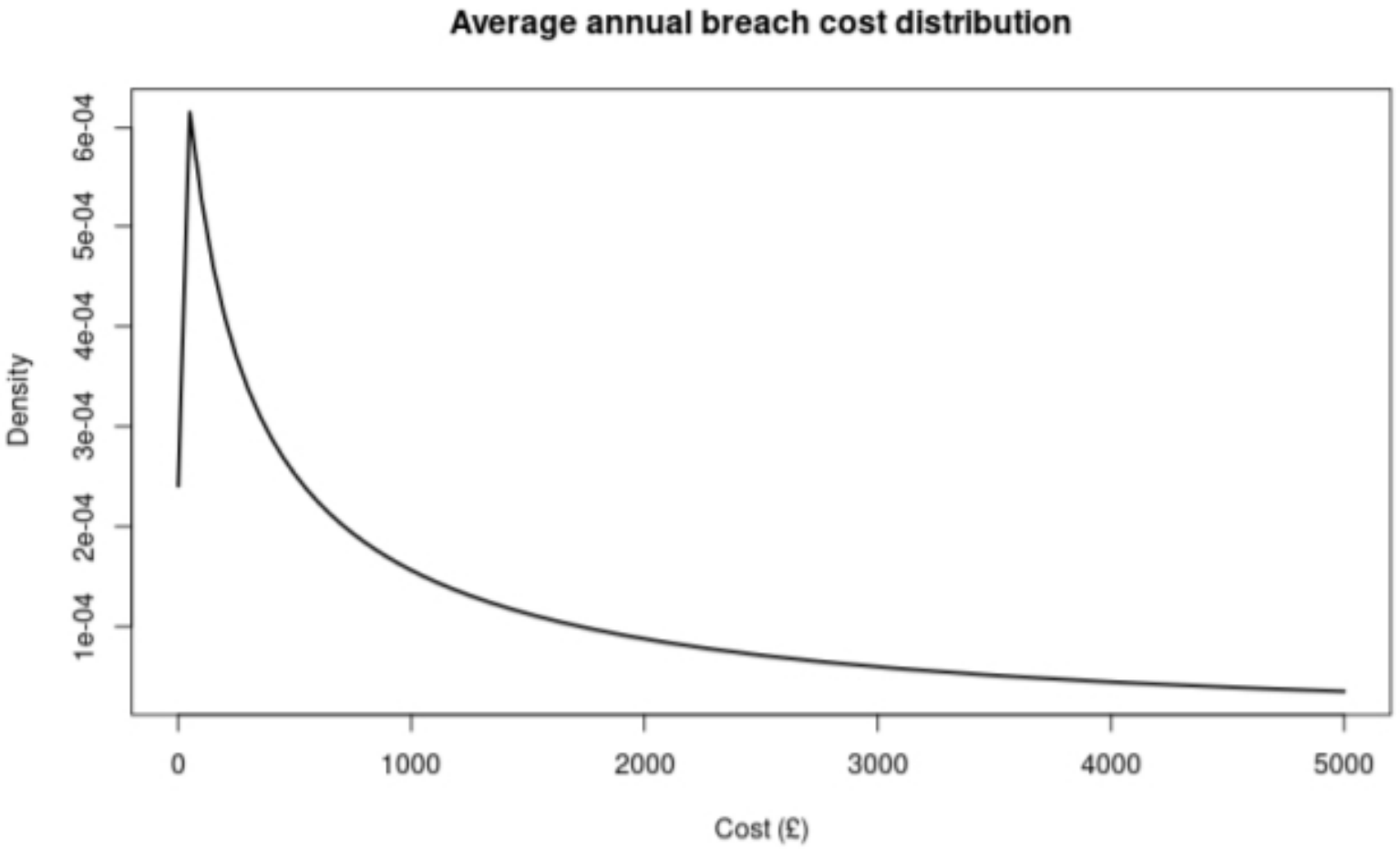
Table 5.1: Average cost of all breaches or attacks identified in the last 12 months[13]

	All businesses
	Only across organisations identifying breaches with an outcome
Mean cost	£3,230
Median cost	£274
Base	160

Real Example
Cost

- To plot log-normal distribution, need mean () and standard deviation ()
- *CSBS* provides the mean (£3,230), which we can use along with the median (, £274) to calculate the , and then the :
  -
  -
  -
  -
  -

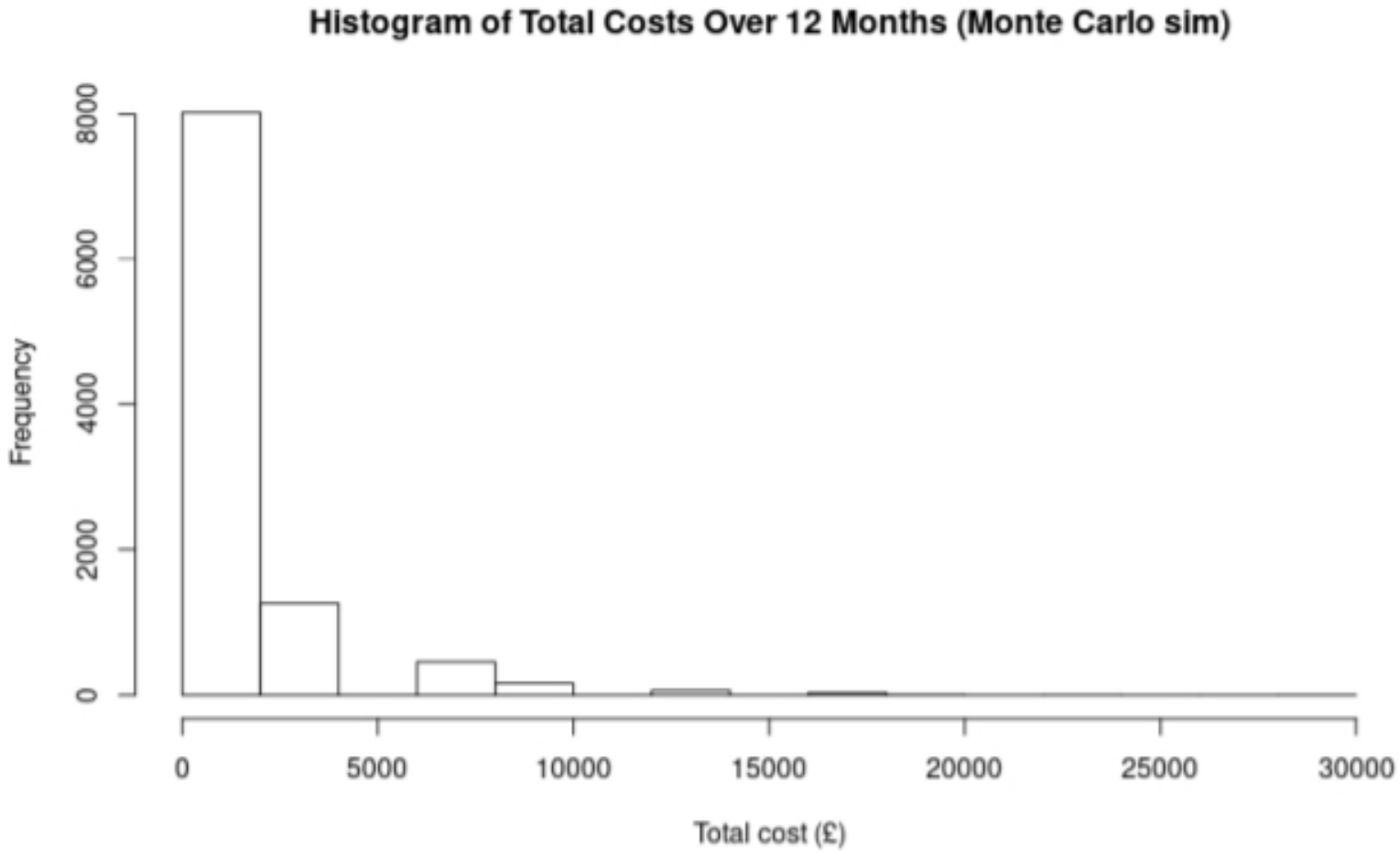
Real Example
Cost



Real Example
Monte Carlo Simulation

- Let = ‘number of attacks’ distribution
- Let = ‘cost of attack’ distribution
-
-
- Annual cost =

Real Example
Monte Carlo Simulation



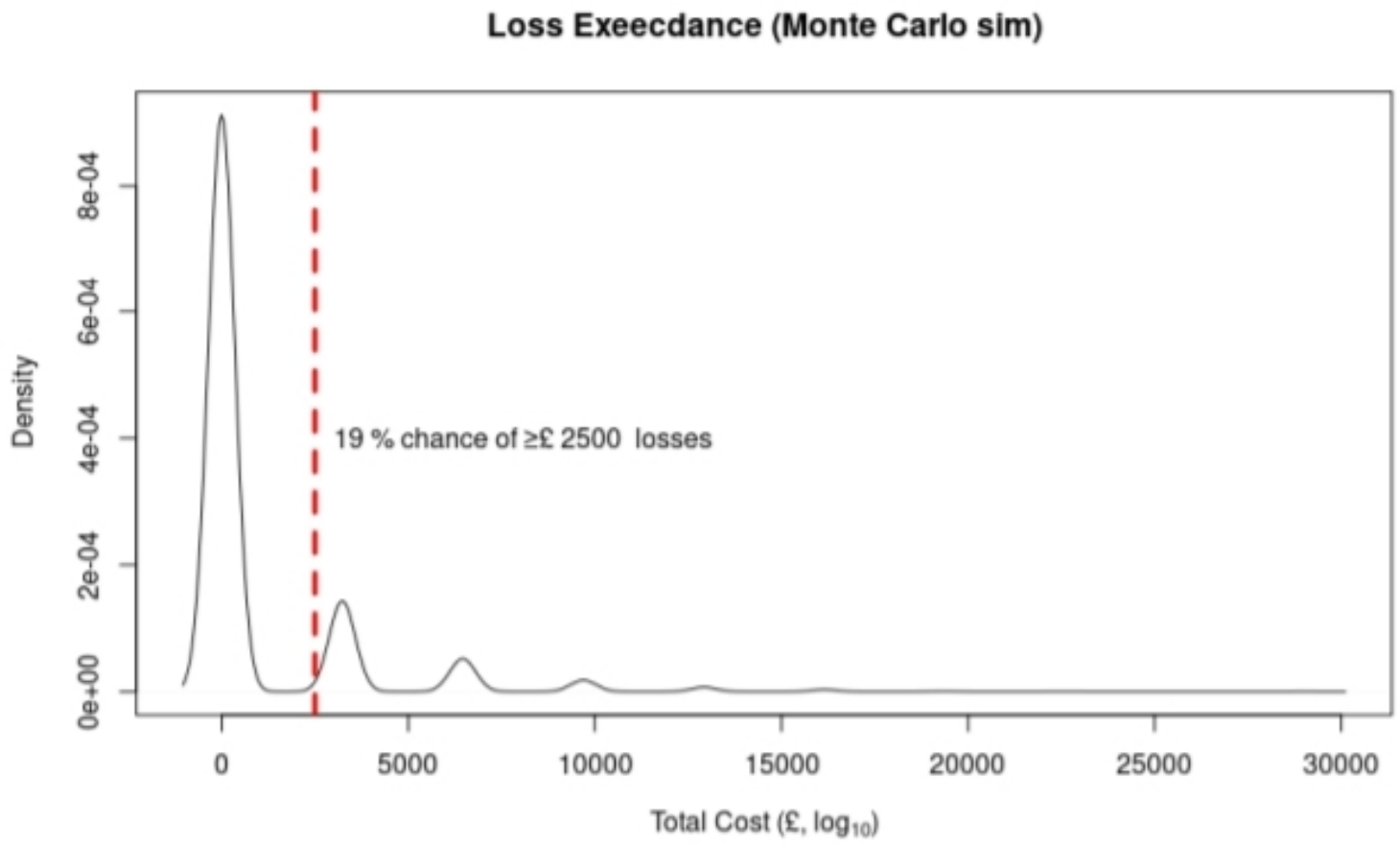
Real Example
Monte Carlo Simulation

§
§
§
§
§

Table 5.1: Average cost of all breaches or attacks identified in the last 12 months[13]

	All businesses
	Across organisations identifying any breaches or attacks
Mean cost	£1,010
Median cost	£0
Base	710

Real Example
Loss Exceedance Curve



Real Example
Other Data in the *CSBS 2020*

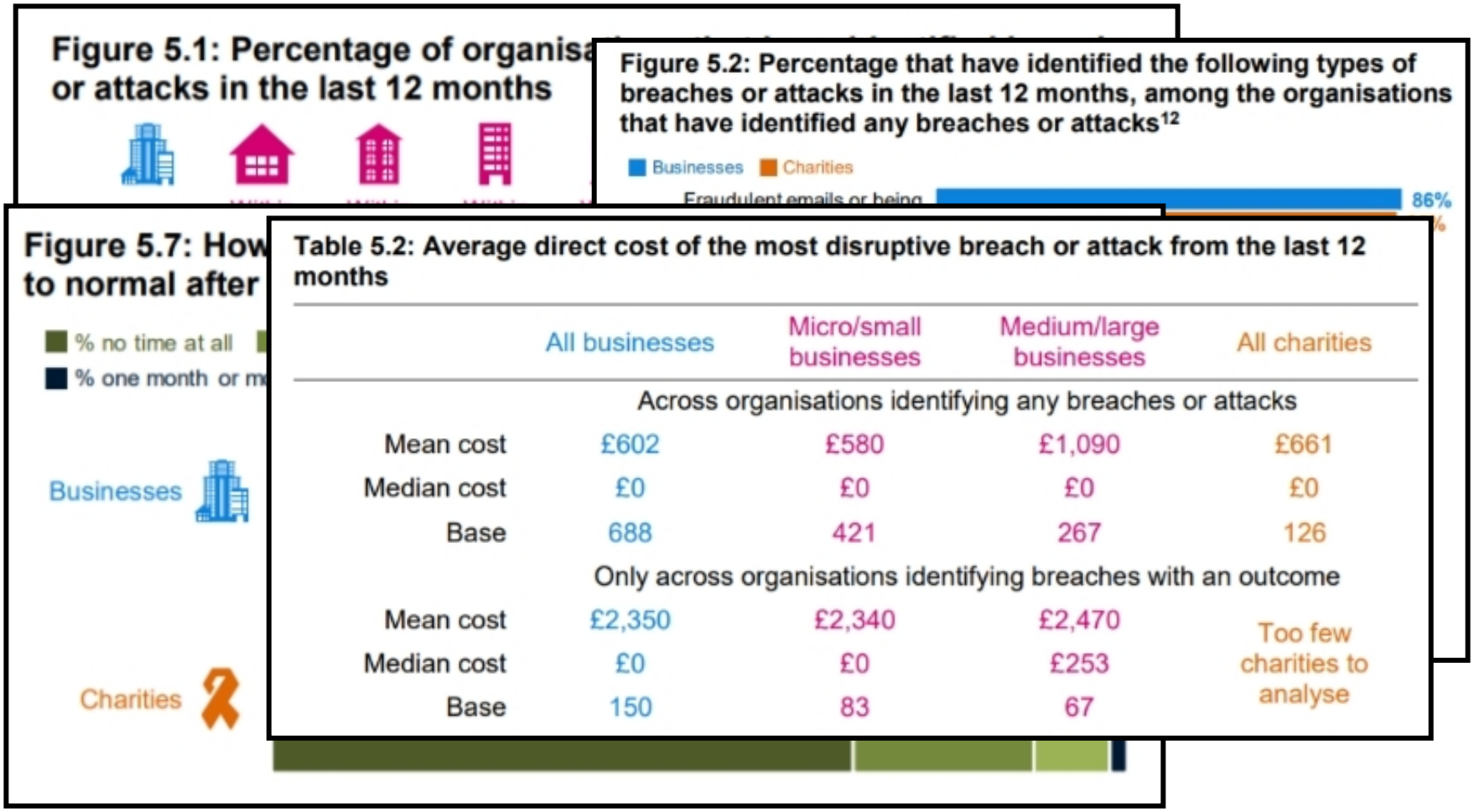


Table 5.2: Average direct cost of the most disruptive breach or attack from the last 12 months

	All businesses	Micro/small businesses	Medium/large businesses	All charities
Across organisations identifying any breaches or attacks				
Mean cost	£602	£580	£1,090	£661
Median cost	£0	£0	£0	£0
Base	688	421	267	126
Only across organisations identifying breaches with an outcome				
Mean cost	£2,350	£2,340	£2,470	Too few charities to analyse
Median cost	£0	£0	£253	
Base	150	83	67	

Wrapping Up

- Non-quantitative methods are **at best** not particularly useful
- Numbers **do not** a quantitative scale make
- If you can't figure out how to measure something, you're **trying to measure the wrong thing**
- You can gain valuable information by analysing **small samples**
- Measurement is not an action leading to a single definitive value, it is a continuous process of progressive **uncertainty reduction**
- Distributions and **Monte Carlo simulations** are your friends

Further Reading

- *How to Measure Anything in Cybersecurity Risk*
  - Effects of the **analysis placebo**
  - Using Bayesian methods
  - Exercises to **calibrate estimation ability**
  - **Decomposition techniques**
  - And a bunch of other neat things!
- My research project
  - Quantifying the impacts and costs of different **control measures**
  - Feeding these into the simulation model
  - **Complex what-if analyses**
  - Provide suggestions on most **cost-effective controls** to implement
  - Message me on Mattermost/email [REDACTED] for more details

Questions, Quibbles, Quomments?