**RISK**

Something that most people DON’T do is weigh out risk and try to put a price on it.

* Everyone has different ways to weight it, but you NEED to do this.
* Saying that something is risky is useless, because everything will have a different relative amount of risk.
* **To be an effective security professional, you need to work out at what point, its worth taking this risk.**
* People are NOT rational risk and are not good at assessing it.
* **We need to think about risk ANALYTICALLY**

Example: the laptop repair shop with world expert catching and throwing parts.

* Maybe there is a 1% chance that they will break a laptop.
* Lets say, the shop serves 40 people and 1/40 of the laptops break.
* It’s not the fact that only 1/40 people were served badly, but 39/40 people were served badly and GOT AWAY WITH IT.
* It was just as bad what happened for those first 39 (the risk that they were put through) as the last case that broke the laptop.

Risk is INVISIBLE, because all we see are OUTCOMES. Because it is invisible, we don’t pay attention to it.

* Humans care deeply about bad outcomes, but are less observant when it comes to risk.
* If the probability is high enough for a bad thing happening, the outcomes you’ll observe are reasonable estimators of the risk. We can make sensible decisions in those cases.
* Humans are great at making decisions about risk when the chance of the bad thing happening is NOT TOO LOW.
* However, when the chance of the bad thing happening is VERY LOW yet the impact of the bad thing happening is CATASTROPHIC, these are the risks that mankind is terrible at assessing.
* WE ARE BAD AT ASSESSING LOW PROBABILITY, HIGH IMPACT EVENTS.
* Because the risk is so low, you may not even see that the risk is there until it happens first time.

In finance, risk is well-understood better than in insurance.

* How is risk priced in finance?
* Essentially, the more risk the asset has, the more reward there will be.
* E.g. If you were offered two assets, with the same expected return but one had more risk (more variance / fluctuation) then the two assets would be priced differently.
* One of the ways of bearing risk, is to shift the cost of risk to someone else.

In the financial world, risk is priced quite well. In security, this is not the case. Why not?

* The volume of trades in the financial market is huge, so if something goes wrong, it is usually something with a relative probability. Past data is a reasonable estimate of what’s going on.
* In the security world, if you’re trying to work out how to protect your firm against something that’s never happened before but is theoretically possible, you have no idea how to assess or weight that up.
* You also don’t know how much money to spend on security. You may spend too much, or too little.
* There is just not enough data to estimate risk.

Hindsight is the best teacher. It is very useful to study instances of low probability events when you can find them and learn from them.  Unfortunately, by definition, this is hard to do in any particular domain since low probability risks rarely occur.

However, although individual instances of low probability risks are hard to spot (chance of me being hit by lightning is low), it is a large large world (there are 4+ billion people at risk of lightning strike) and there are many many different types of low probability events at risk (struck by lightning, golf ball, earthquake, find gold nugget, ...) so by keeping your eye on the news you can invariably learn about quite a few which have occurred each week.  Learn from earthquakes, bridge collapses, oil rig failures, pandemics etc so you can better assess risks of security failure in your own particular domain.