The Cybersecurity Paradox, what is it?

A paradox is making an irrational decision given a set of rational choices, or as I like to think of it as,

What in the world!

There are classic examples of paradoxes, e.g., the

Allais Paradox:

In deciding two possible outcomes below, people will choose choice 1 in experiment 1.

However, it doesn't matter which you choose – yet.

Experiment 1	
Choice 1	Choice 2
100% to win 24,000	97% to win 27,000
	3% to win nothing

In experiment 2, people will choose either choice 1 or 2, and again, it doesn't matter - yet.

Experiment 2	
Choice 1	Choice 2
34% to win 24,000	33% to win 27,000
66% to win nothing	67% to win nothing

The problem is when you have to make both decisions at the same time, that is experiment 1 and experiment 2. In that case, the majority of people will choose choice 1 in experiment 1, and choice 2 for experiment 2 – this is the paradox and the problem.

In Expected Utility theory, people choose to get the most value.

However, when calculating the Expected Utility of experiment 1 and experiment 2, it is

However, I do not see this as irrational thinking – it's normal thinking, we throw money at a lot of things. Government projects, company investments, I have a 95 Subaru that I love and keep throwing money at it to keep it running (The framing loss effect)

There is also a lot of discussion on privacy vs. security paradox, but again, that's a decision, do you want more security, less privacy, or less security, more privacy.

A privacy vs. security paradox would be you have two choices to make, and in one choice you choose (more security, less privacy), and in the second choice you choose (less security, more privacy)

However, you advocate for (more security, less privacy), that would be the paradox, you want the maximum utility, but your decisions do not reflect your desire.

So, what's the Cybersecurity Paradox?

Given two experiments, in the first experiment, where does your company spend most of its cybersecurity investments?

Experiment 1	
Choice 1	Choice 2
Technical solutions	Human behavioral solutions

Respondents answer choice 1; we spend hundreds of millions of dollars on technical solutions to cybersecurity issues.

The next question is where do you think the biggest problems in cybersecurity are

(experiment 1, choice 1) and (experiment 2, choice 1) that have the most utility, but people will choose (experiment 1, choice 1 and experiment 2, choice 2), thereby creating the paradox, i.e., not choosing the one with most utility, or value to them.

(It's a math thing)

So, in choosing (experiment 1, choice 1) and (experiment 2, choice 2), you get less expected utility or value, but that is not what you want.

Ellsberg paradox:

Another famous paradox looks at the way people view odds. A risk of 0% to 1%, is not viewed the same as the risk from 1% to 2%, or the risk from 22% to 23%, or the risk from 99% to 100%. If we asked people to rate the importance of these changes in percent on a scale of 1 to 10, how would they rate them?

A change of 0% to 1% rated as 1, least important, but a change of 89% to 90% rated as an 8, almost the maximum importance.

Percent Change	Impact of % change on a
	Scale of 1 to 10
0% to 1%	1
1% to 2%	1
2% to 3%	1
35% to 36%	2
74% to 75%	4
89% to 90%	8
99% to 100%	9

However, all these are all the same risk levels; it's just a one-percent difference, so we don't base our decisions, well, rationally. We see a jump of 89% to 90% as being much more important than a jump of 1% to 2%.

Experiment 2	
Choice 1	Choice 2
Cybersecurity problems are caused by technology	Cybersecurity problems are caused by humans

Most of the same respondents on experiment 1, who picked choice 1, now in experiment 2 would pick choice 2, it's a people problem.

The same results of the Allais Paradox, i.e., picking less expected utility or value.

This is not to blame anyone, in a car crash, is it the automobile, or the driver the cause of the crash? A truck crash, plane crash, etc., most often a set of events that should have been caught were missed, so when someone fat-fingers an email, remember, there was a chain of events that led to that fat-fingering.

Look up the great electrical blackout of 2003 when the east coast went dark; it was traced back to a fuse. The non-malicious end-user was not the problem; the end-user was just unlucky enough to be at the end of the chain of events (but yes, we do have malicious end-users unfortunately)

Can we explain the Cybersecurity Paradox?

Possibly, one reason is the same as with the Allais and Ellsberg paradoxes in that human just think irrationally, we let emotions interfere, and when given choices we mix them. For example, if we are given a set of choices to make, we sometimes assume they are all related and have to look at them as a whole (Gestalt laws)

Second, it also relates to Return on Investment (ROI). In a technical cybersecurity solution, I can gauge some ROI now, the value of the equipment, or the number of attacks this equipment is supposed to stop. All these

And this helps to explain why people would run to play a Mega-Millions lottery where their odds are extremely high against winning, vs. a much smaller lottery, but having better odds, but paying less. Researchers try to explain this in different ways, e.g., people tend to go for the sure thing, e.g., In experiment one, I know I have a 100% chance to win 24K dollars. In experiment two, both choices stink, I have a 66% and 67% chance of losing, so hey, why not, let's go for it all, what can I lose. These paradoxes point out the fragility of emotions on human decision making, so Maybe Spock was right after all. That brings us to the Cybersecurity Paradox. I have read a lot of research about what exactly is a Cybersecurity and Paradox. A lot of it comes down to money and that we are just throwing money at the problem.	data points help me to close my thinking on ROI, and allow me to feel good basically. Yes, making decisions does make us feel good if it brings closure. But not so in human behavioral solutions, we have to guess, make assumptions and hope our investments pay off – and that destroys our cognitive balances. However, that would be folly, since we do have data points. Password policies have reduced unauthorized entries, awareness on piggybacking have reduced multiple people walking in together, social engineering training has reduced those failing to its grasp. Sure, there is more to do, but investments in people help. So, in making decisions, cybersecurity experts need to understand these paradoxes exist and will interfere with their decision making. Allais, M. (1953). Le Comportement de l'Homme Rationnel devant le Risque: Critique des Postulats et Axiomes de l'Ecole Americaine. (The Rational Man's Behavior in the Face of Risk: Criticism of Postulates and Axioms of the American School). Econometrica, 21(4), 503-546. Ellsberg, Daniel (1961). Risk, Ambiguity, and the Savage Axioms. Quarterly Journal of Economics. 75 (4): 643–669. doi:10.2307/1884324. JSTOR 1884324.