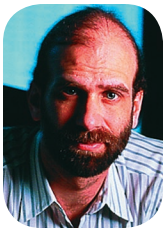
How the Human Brain Buys Security

People tend to be risk-averse when it comes to gains, and risk-seeking when it comes to losses. If you give people a choice between a $500 sure gain and a coin-flip chance of a $1,000 gain, about 75 percent will pick the sure gain. But give people a choice between a $500 sure loss and a coin-flip chance of a $1,000 loss, about 75 percent will pick the coin flip.



Bruce Schneier
BT

People don't have a standard mathematical model of risk in their heads. Their trade-offs are more subtle, and result from the way our brains have developed. A computer might not see the difference between the two choices—it's simply a measure of how risk-averse you are—but humans do.

This fact might not seem like a big deal, but it overturned standard economic theory when it was first proposed in 1979. It's called "prospect theory," and was developed by Daniel Kahneman and Amos Tversky to explain how people make trade-offs that involve risk.

Evolutionarily, it makes sense. It's a better survival strategy to accept sure small gains rather than risk them for larger ones, and risk larger losses rather than accept smaller ones. Lions, for example, chase young or wounded wildebeest because the investment needed to kill them is lower. Mature and healthy prey would probably be more nutritious, but there's a risk of missing lunch entirely if it gets away. Because animals tend to live on the razor's edge between starvation and reproduction, any loss of food can result in death, and the best option is to risk everything for the chance of no loss at all.

This cognitive bias, demonstrated again and again by many researchers—across ages, genders, cultures, and even species—is so powerful that it can lead to logically inconsistent results. Google "Asian disease experiment" for an almost surreal example. Describing the same policy in two different ways, either as "200 lives saved out of 600" or "400 lives lost out of 600," yields wildly different risk reactions.

Prospect theory explains one of the biggest problems our industry has with selling security: no one actually wants to buy it. Salespeople have long known there are basically two motivations to get people to buy: greed and fear. Either buyers want something—and thus spend to get it—or don't want something, and spend to help prevent it. It's much easier to sell greed than fear.

Security is a fear sell. It's a choice between a small sure loss—the cost of the security product—and a large risky loss—the potential results of an attack on a network. Of course, there's a lot more to the sale. Buyers must be convinced that the product works, and they must understand the threats and the risk that something bad will happen. But all things being equal, buyers would rather take the chance than buy the security.

Sellers know this and are continually trying to frame security products in positive terms: slogans like "We take care of security so you can focus on your business," or carefully crafted ROI models that demonstrate how profitable a security purchase can be.

Another option is to push the fear button really hard. Our brains might prefer risky large losses to sure smaller losses, but when we're really scared we'll do almost anything to make that feeling go away. In our industry, we call it FUD—fear, uncertainty, and doubt. We've seen fear alter the political landscape in several countries following the 9/11 terrorist attacks.

The better solution is not to sell security directly, but to include it as part of a more general product or service. Your car comes with safety and security features built in; they're not sold separately. And it should be the same with computers and networks. Vendors need to build security into the products and services that customers actually want. Security is inherently about avoiding a negative, so you can never ignore the cognitive bias embedded so deeply in the human brain. But if you understand it, you have a better chance of overcoming it. □

***Bruce Schneier** is chief security technology officer of BT. Subscribe to his email newsletter, Crypto-Gram, at www.schneier.com.*