Cyber Security and the Probability Challenge

Reframing the cyber investment imperative

It's summertime. The sun is shining. A warm breeze is blowing. And you're about to dive into a big bowl of ripe, red strawberries. You can picture it, right?

Now try to picture a million strawberries. Or how about a billion. Not as easy, is it? Whether a million or a billion, that many strawberries start to mesh together and look the same. That's because humans weren't designed to visualize those kinds of whopping numbers. In fact, an old joke among cognitive scientists says that we humans count like this: “One, two, three, many.”

As it turns out, because humans are cognitively challenged at counting large numbers, we’re also not so good at probability analysis. Absent real-world metrics, can we really conceptualize the difference between one in a million versus one in a billion? If your answer is, “Of course we can,” then think again about visualizing the difference between a million strawberries and a billion strawberries. For us humans, large probabilities become fuzzy very quickly.

We humans count like this: "One, two, three, many."

Yet executives and cyber practitioners are tasked with making security decisions where the probability of occurrence is the key variable in both the amount of investment and concern.

Looking at a real-world example, let’s say there is a one in 100 million chance that a particular piece of industrial equipment will be attacked. If a factory has 100,000 pieces of equipment, does that mean, by extrapolation, that there is a one in 1,000 chance that at least one of those pieces will be attacked? What if the probability analysis is off by a factor of 10, or worse, a factor of 100? What if instead of factories, we start looking at Industrial Internet of Things (IIoT) devices, where there may be millions deployed? It quickly becomes mind-boggling. With 50 billion devices expected to be connected to the Industrial Internet by 2020, assessing risk with large numbers is no longer an academic exercise.

While the probability of attack against industrial environments is an on-going discussion, what we do know is that many operational technology (OT) and IIoT devices are vulnerable to attack. We also know that nearly 70% of utility, oil and gas, manufacturing, and energy companies reported at least one security breach in a 12-month period[1], and that 78% of organizations with ICS/SCADA environments expect a successful exploit over the next 24 months.[2]

1 *Barron-Lopez, L., “Cyber Threats Put Energy Sector on Red Alert,” TheHill.com, July 15, 2014.*

2 *Critical Infrastructure: Security Preparedness and Maturity, Unisys and Ponemon, July 2014.*

Yet business decision-makers are still finding it difficult to agree on exactly what the probabilities are. Lack of clarity makes it hard for organizations to move forward with effective risk mitigation. “We have to do something” is often the consensus, but how much and how quickly relies on uncertain assumptions about risk.

No doubt, if a power company’s leadership team could walk into a board meeting and say with certainty that there is a 10% chance that a plant will be attacked within the year, and that the attack will result in two weeks of unplanned downtime and loss of human life, the board would say, “Tell us what’s needed to prevent that from happening.”

But if the same team were to go in and say, “We’re not sure. There’s maybe a 0.1% chance of something bad happening,” they wouldn’t be making a great case for investing in security.

Organizations may know who the threat actors are, why they attack, and what the potential impact of attacks are. But the probability of being attacked, especially if they’ve never been attacked before can be difficult to grasp. And therein lies one of the inherent challenges of trying to make a business case for investing in security

Assurances vs. losses

There is an economic theory around how humans make risk-based decisions that tells us a lot about cyber security decision-making. In 2002, psychologist Daniel Kahneman won the Nobel Memorial Prize in Economic Sciences for his groundbreaking research on the prospect theory that identified an inherent, genetic behavior in the area of decision-making under uncertainty. Via a straightforward experiment, he was able to demonstrate how people make decisions around risk, finding that most are risk-averse with respect to gains and risk-seeking with respect to losses.

The experiment, which has been replicated many times over with different demographics and across diverse domains, has always shown extremely close and regular results. This is how it works:

A room full of people is divided into two groups. The first group is given this choice: would they rather receive a guaranteed $100 right now? Or would they prefer to flip a coin and take a 50-50 chance of getting $150 or winding up with nothing?

The second group is asked to make a different choice: Told that the government has just introduced a new tax, they are asked to choose to pay $100 straight away. Or they, too, could flip a coin and take a 50-50 chance of having to pay $150 or nothing at all.

In group one, approximately 75% of participants will consistently choose to keep the $100 and not take the chance. In group two, approximately 75% of participants will decide to take a chance and flip the coin.

As Kahneman has written, “For most people, the fear of losing $100 is more intense than the hope of gaining $150.” [3]

3 *Daniel Kahneman, Thinking, Fast and Slow, (New York: Farrar, Straus and Giroux, 2011), 284*

There has been much analysis around these results. You can change the terms, the vocabulary, the people, but what Kahneman did, and the reason he earned the Nobel Prize, was that he showed that humans are willing to gamble 75% of the time on a potential loss; but also willing to keep a sure thing 75% of the time.

Kahneman believed the choices had to do with evolutionary biology. If we think about how cavemen survived, they were likely better off getting a little bit of food and guaranteeing survival than taking a chance on not eating anything at all. In other words, they were better off chasing a smaller animal, eating what they could, and only running when a predator or other risk of danger appeared.

That's why most of us are willing to flip a coin in terms of how much, when, and where to invest on cyber security. Some organizations might say, "Even if you tell me I'm vulnerable, and even if I understand and agree a 100% about the probable risks around connecting my assets, the potential vulnerability of my equipment, and the possible shortcomings of a slow change-management lifecycle, I've never been attacked, so why should I worry?

If organizations have not experienced a significant attack, it is difficult to tell them they need to deploy a certain security solution. Even if they were told, with perfect accuracy, of the probability of an attack, 75% of the time they would still roll the dice, take a chance, and not purchase security.

But what if organizations were to begin to think of security in terms of preserving gains and ways they could instill confidence with their boards that production and operational processes were working effectively?

Prospect theory suggests that while we may be reluctant to invest in cyber security to prevent losses from a hypothetical attack that might not happen, we are much more likely to invest to help achieve a desired, positive outcome. By recognizing that a bird in hand is always more desirable than a 50% chance of two birds in a bush, organizations can now reframe the cyber investment imperative to one of confidence.

About GE

GE (NYSE: GE) is the world's Digital Industrial Company, transforming industry with software-defined machines and solutions that are connected, responsive and predictive. GE is organized around a global exchange of knowledge, the "GE Store," through which each business shares and accesses the same technology, markets, structure and intellect. Each invention further fuels innovation and application across our industrial sectors. With people, services, technology and scale, GE delivers better outcomes for customers by speaking the language of industry.

Contact Information

Americas: 1-855-YOUR1GE (1-855-968-7143)
gedigital@ge.com

www.ge.com/digital