Cybersecurity Risk Management using Leading and Lagging Indicators

Most CISOs would agree that quantifying cybersecurity risks using potential impact and likelihood is a numbers game; no two people will come with the same risk numbers using this formula. Is there a better way to understand cybersecurity risk? How about if we classify all cybersecurity risk in terms of Leading or Lagging indicators?

People in the financial and banking risk management world do this every day. One of the common topics that get discussed on CNBC, in the Wall Street Journal, and by hedge fund gurus is managing risk using leading and lagging indicator. Also, how they use these two indicators to make financial risk management decisions. These days one of the most common recession risk measurement that gets discussed is the potential inversion of short-term rates above the longer-term rates; a leading indicator of a pending recession. We don't have a recession yet, but it is almost like we can predict when one will happen. Maybe it is time for cybersecurity folks to use what financial gurus have been using for a long time to anticipate better and manage risk; Leading and Lagging indicators.

It is not that difficult. When you exercise every day, it is a leading indicator of your health, but when you fall sick or have a heart problem because you choose to watch TV all the time it is a lagging indicator of your health. If you already have the problem - it is a Lagging indicator.

The number of times you were hacked or the number of compliance finding you had this quarter is a lagging indicator. It is done, almost too late. You cannot change the course. How about we look for risk metrics that will allow us to impact the outcome; Leading indicators.

According to the Cloud Security Alliance website "A lagging indicator measures actual results, outputs, so it's too late to make a correction or improvements. A leading indicator looks at activities necessary to achieve your goals, so they are essentially inputs that provide information needed to intervene and change course for the better."

Having had the opportunity to work as summers undergraduate intern, two years in a row, and after discussing with some of my classmates who worked at different companies in the summer, I can say for sure that not many companies classify Operational and Regulatory risks using Leading and Lagging indicators. They present cybersecurity risk metrics, "the top ten risks we have." and how we plan to work on all of them. Could we be missing an opportunity to manage risk and risk investments?

I would recommend that cybersecurity teams should focus on differentiating Leading and Lagging indicators prior to deciding on risk treatments and investment they make. A greater focus on leading indicator could potentially help better manage cybersecurity and regulatory compliance risks.