IS ROI/IRR/NPV A GOOD MEASURE FOR CYBERSECURITY?

In God We Trust; Everyone Else Bring Me Data

The standard dogma of the management business community is "if you can't measure it, you can't fix it" or rather, "don't take on any project where you don't have numeric metrics." C-Level Staff, managers, and employees do not do very well with ambiguity; that is, not being able to directly equate costs and benefits to numbers. This ethos is reinforced by two factors:

1. From the internal management side, it's much easier to track progress and effectiveness with solid numbers
2. Form the external side, it is easier to measure how effective investments numerically and comparatively

In many ways, this ROI system works. In the corporate finance world, the first of three responsibilities for a CFO is to find positive Net Present Value (NPV) projects to invest in (the other two being: (2) deciding on and maintaining the ratios of debt to equity and (3) deciding what share of profits to reinvest and what to payout). The NPV formula here takes the cash flows (negative at the onset of a project but then presumably increasing and positive after a few months/years), discounts them by a factor (that considers the time value of money as well as the efficiency of the firm), and finally sums them up. If a project is then NPV positive, it is worth doing. The Internal Rate of Return (IRR) is then determined by calculating the discount rate that would make all NPV Cash Flows negative. The quicker and more profitable the project, the higher the IRR and the better your investment or company or project becomes.

The Issue: Measuring Risk

The fundament problem with these measurements is that they are calculated based on future estimates. Yes, with years of experience and data one can get better and better at finding trends and minimizing variance between predictions and actuals, but this is mostly achieved during what this author would call, non-tumultuous times. The best evaluators (the Aswath Damodaran's of the world) all bring in other non-firm-specific factors into their models. Undiversifiable Risks, these are the "rising tides which lift all boats" (á la the financial crash in 2008 or the emergence of high value unicorns), are extremely difficult to predict with historical data (even if you are inside the industry).

The financial crisis of 2008 lead to lower cash flows than predicted for virtually all firms whereas the emergence of tech unicorns like Facebook and Uber are being purchased and finance at levels higher than their evaluations. Both events are sentinel but nonetheless distort previously time-tested models. Additionally, although these black swan events (high impact low probability) are rare, there is a shifting school of thought that predicts that these events (which can be many standard deviations away from the mean occurrences) are actually much more likely to occur than previously predicted. Rather than thinking of all possible events as having a normal distribution (where probability of rare events is extremely small) many believe that the actual distribution of possible events in the world follows a Power Law or Fat Tail distribution. This framework suggests that, while still not likely, the chance of these rare events occurring is not negligible:

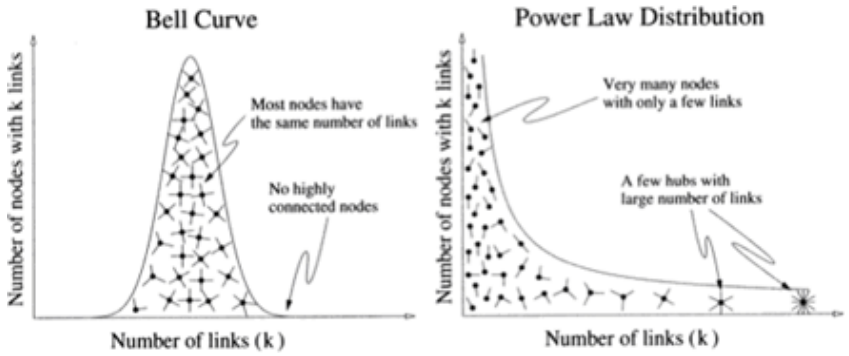

Figure 1 - Retrieved From http://edgeperspectives.typepad.com/edge_perspectives/2007/05/the_power_of_po.html

The Farma-French Model wins the Nobel Prize in the 90s by adding the three factors to the Capital Asset Pricing Model (CAPM): (1) Size of Firm (2) Price/Book Ratio and (3) Market Risk. This new model is now deemed more accurate (albeit more painful to calculate) precisely because it attempts to take more external factors to diversify away the risk of giant market events. Cybersecurity attacks are akin to these sentinel market collapses – rare yet devastating. The Farma-French Model was amended in 1997 to the Carhart 4 Factor Model by adding a new variable of *Momentum*. A future Noble prize will be awarded to economists, mathematicians, or financial engineers who will improve this model in order to properly price risk into investments.

The traditional method of ROI is just not equipped to accurately price in cataclysmic market alerting events which is why it should not be used in a cyber security analysis. Efforts such as a standard risk management assessment (weighted averages assigned to different assets and analyzing the probability and devastation of an attack) are important tools, but only insofar as they are able to get the conversation going at the management level. The numbers produced by each technique are virtually worthless when taken individually.

Future Notes

The logical extension here is: if not NPV/IRR based metrics, how can one successfully and repeatedly evaluate and price cyber security risks? One solution could be the Asset Pricing Model in finance: just keep adding more and more variables to get a more fine-tuned equation. Others, mostly at smaller companies, conclude that it's not even worth the investigation (because of the low likelihood of attack). Whatever is going to be done however, must come (or be forced upon) the private sector.

Upwards of 85% of all critical technological infrastructure and capabilities are owner by private enterprise. When looking at global solutions to the cybersecurity pricing dilemma (and one must look globally because of the broad geography of attack locations) real change will come from the private industry. Governments, if they are able to identify vulnerabilities in multinational corporations, or in other governments, have a military advantage to keeping their mouth shut. North Korea certainly didn't hack Sony under the premise of alerting them to their security weaknesses. These problems are additionally going to be compounded with advancements in smart infrastructure (e.g. smart energy grid) and the Internet of Things (IOT) where virtually all devices are going to be put online.

One final note is that the true extent of the power and extent of cyber attacks and war is that we haven't seen yet their true power. The BotNet and DDoS attacks featured in the Russia-Georgia Cyber War are

generally on the lower end of potency spectrum. A more Stuxnet approach of using code or software to cause physical damage (i.e. blowing up an oil refinery) absolutely exists, yet the world hasn't really seen it yet. Official State on State Cyber Warfare akin to a World War hasn't occurred yet. Traditional measures of ROI and IRR cannot equate for these future realities. They are merely tools used by management to attract investment, evaluate and execute projects, and to turn VP's into CEO's and CEO's into Board Members.