For Good Measure

The Price of Anything Is the Foregone Alternative

DAN GEER AND DAN CONWAY

Dan Geer is the CISO for In-Q-Tel and a security researcher with a quantitative bent. He has a long history with the USENIX Association, including officer positions, program committees, etc.
dan@geer.org

Daniel G. Conway is founding director of the MBA in Analytics program at Loras College and is a faculty member in the McCormick School of Engineering at Northwestern University. He previously served on the faculty of Indiana University and the University of Notre Dame.
daniel.conway1@northwestern.edu

Cybersecurity insurance has been talked about forever, but absent some ill-advised government mandate, the insurance market is not going anywhere useful without better data.

A demand for insurance emerges as soon as traditional risk management providers of family, clan, and tribe become too small to help. The first formal insurance was supplied to enable risk transfer around physical assets, which are susceptible to harm by physical forces.

In Nature, physical forces are local. Physical risk mitigation strategy thus requires pooling of risk based on locality independence. For example, the risk of a fire in NY is uncorrelated with, and thus offset by, the risk of a typhoon in Taipei, which is uncorrelated with, and thus offset by, the risk of an earthquake in Istanbul. A successful insurance company diversifies risks geographically so as to remove the impact of the correlation implied in locality. You don't write fire insurance for abutting tenements.

In information security, locality is manifested by systems which, when compromised, have a correlated impact on value. These systems include operating systems, ubiquitous applications, standardized protocols, and a host of other vulnerable single points of failure. For any operating system code base, all instances of it are "virtually local." In essence, this means we have only a few digital cities, each built within the digital world's "ring of fire." Insurance providers cannot offer affordable insurance without a means of diversifying locality, that is to say without limiting the provider's own exposure to cascade failure among their insureds.

In a recent DHS workshop on cyber insurance [1], many suggestions were offered to drive adequate coverage alternatives and thus maturity in the cyber insurance industry. The report cited the difficulty insurance providers faced:

1. a lack of actuarial data, which requires high premiums for first-party policies that many can't afford;
2. the widespread, mistaken belief that standard corporate insurance policies and/or general liability policies already cover most cyber risks; and
3. fear that a so-called "cyber hurricane" will overwhelm carriers who might otherwise enter the market before they build up sufficient reserves to cover large losses.

Difficulty (3) results from locality, so an insurance company would prefer to provide coverage for potential insureds that have system diversity. This can be encouraged through discounts for those with diverse system characteristics and verified through audit or embedded monitoring tools. Difficulty (2) is beyond the scope of this column. We focus on difficulty (1), which has been at the heart of For Good Measure since its inception (http://geer.tinho.net/fgm).

The most reflexive strategy to collect better actuarial data is to impose data sharing through regulation, and that approach can have positive results if accompanied by liability protection; however, the incentives for reporting events completely and accurately are generally unaligned with the organization's individual reward structure, viz., full disclosure exposes firms to litigation and potential additional cyber risks that far exceed any value to be gained from such disclosures. Moral hazard has a digital counterpart.

Year	Incidents
2005	156
2006	643
2007	774
2008	1048
2009	727
2010	828
2011	1088
2012	1586

Table 1: Data Loss Events per Year

A Market Approach

A market approach would induce sharing of actuarial data by providing a framework for rewarding contributed value, which would, as a result, provide inference into event trends. Rewards tend to attract further market participants, often resulting in the maturing of metrics programs and improved management techniques. Analytics in baseball has been good for maturing baseball. Analytics in the cyber insurance industry would catalyze maturation in cyber risk management and are a necessary component of re-insurance.

What would such a market look like, and how might it be used to improve security? A participant in the DHS workshop described (1) the frequency and (2) the severity of events as the "Holy Grail" of cybersecurity risk management, so we start with that. Severity is in the eye of the beholder, and thus subject to stakeholder appetite for risk. Financial markets use spot price of money for this measure, and ignore the beholder's current position and/or money demand. Futures markets and money markets extend the spot concept to a price-over-time concept, and thus allow for better capital planning. (Time-lapsed pricing permits the incorporation of data points, such as the frequency of certain events occurring over time, that spot pricing cannot capture.)

What would a market for "event frequency" as a commodity look like? For data, we take 96 months of event frequency, from 2005–2012, using the Data Loss Database [2] as a proxy. Events by year are represented in Table 1, and events by month in Figure 1.

Financial analytics professionals have created markets to buy and sell probabilities for many domains, including who will be the next president, the next pope, and the next winner of "Dancing With the Stars." During the most recent MIT sports analytics workshop [3], major league baseball teams suggested that their players were evaluated as if they were financial assets and a team was a portfolio of such options on those assets.

If changes in cybersecurity event frequency were important to us, we could treat that frequency as if it were a financial asset,

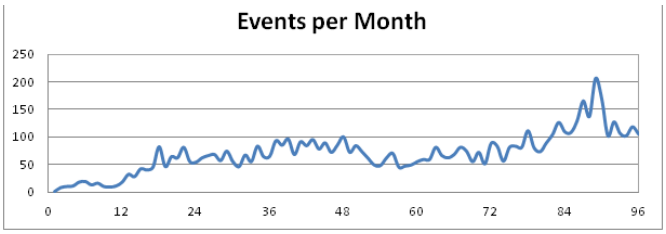

Figure 1: Data Loss Events by Month (2005-2012)

and, more importantly, we could price futures in cybersecurity event frequency. For our example, we will use ticker symbol XEF. This market could be used as a hedge against risks for those most susceptible to an increase or decrease in event frequency, such as cyber insurance providers. Increases in XEF "price" would mean that the market predicts an increase in the frequency of cybersecurity events.

For example, if an email company were measuring the frequency of ".exe" attachments over time and saw a spike in that metric, they could purchase shares of XEF in anticipation of an increase in future cybersecurity events. Any market participant who was sensitive to an increase in such events might purchase an option to buy XEF in the future for a small price today as a risk mitigation instrument. This market would likely be more responsive in terms of expectations than data collected through regulatory imposition.

Option Pricing via Black-Scholes

Black-Scholes option pricing [4] is a widely used calculation method in finance for providing future price information on assets, and is used to price grain futures, weather futures, and the value of major league baseball players. In our case, it would have a price on the future of XEF, that is to say the future frequencies of cyber events. A mature options market in XEF would allow a market participant to purchase the right (but not the obligation) to buy XEF in the future at a set price in exchange for an amount today. Such prices are determined by the volatility of the underlying stock where, in the case of XEF, the underlying is security debt as defined by Wysopal [5].

To be concrete, and again using the monthly data from datalossdb.org as a proxy, if the investor wanted to obtain the right to purchase (call) a share of XEF at a price of 90 in three months from December of 2012, the investor would identify the following:

- Spot price today: 106
- Future strike price: 90
- Risk-free rate (historical monthly increase): 1%
- Volatility: 27%

Months	Call	Put
1	$ 21.00	$ 4.10
2	$ 25.24	$ 7.45
3	$ 28.68	$ 10.02
4	$ 31.65	$ 12.12
5	$ 34.28	$ 13.89
6	$ 36.68	$ 15.44
7	$ 38.88	$ 16.79
8	$ 40.92	$ 18.00
9	$ 42.83	$ 19.09
10	$ 44.63	$ 20.06
11	$ 46.33	$ 20.95
12	$ 47.94	$ 21.76

Table 2: Call and Put Option Prices for XEF

The Black-Scholes calculation would then price at 28.68 (dollars) the option of purchasing a share of XEF in three months at 90 (dollars). Table 2 lists various option prices for a future price of 90. We also include the price for the option to sell (put) a 90 (dollar) share of XEF in the future.

A futures market for event frequency in cybersecurity might offer a way for security professionals to infer future events as well as provide a mechanism to insure against the associated risks. The amount we invest in future calls/puts reflects our perceived impact of an event, thus pushing the severity half of the Holy Grail metric to the beholder.

John Poindexter and others demonstrably understood the potential of derivative markets to serve as predictors of future events, although they were unable to navigate the political obstacles to realize such markets [6]. Now is the time to revisit those ideas; cybersecurity is in crisis, and crises must not be allowed to go to waste.

References

[1] Cybersecurity Insurance Workshop Readout Report: http://www.dhs.gov/sites/default/files/publications/cyber-security-insurance-read-out-report.pdf.

[2] DataLossDB: http://datalossdb.org/.

[3] MIT Sloan Sports Analytics Conference: http://www.sloansportsconference.com/.

[4] Investopedia: http://www.investopedia.com/terms/b/blackscholes.asp.

[5] C. Wysopal, "A Financial Model for Application Security Debt": http://www.veracode.com/blog/2011/03/a-financial-model-for-application-security-debt.

[6] R. Hanson, "The Policy Analysis Market: A Thwarted Experiment in the Use of Prediction Markets for Public Policy," Innovations, Summer, 2007: http://hanson.gmu.edu/innovations.pdf.