

Nothing Ventured, Nothing Gained

It is not because things are difficult that we dare not venture.
It is because we dare not venture that they are difficult. —Seneca, ca. 50 A.D.

Cybersecurity seems always to be just minutes away from some really smart security metrician elegantly capturing a unified field theory for valuing security, thus ushering in the gilded age of rational cybersec. In the meantime, the pessimistic—

a go of being entrepreneurs, the time from inception to IPO has risen from 4.9 years in 2000 to 8.4 years today, while the odds against an IPO have become all but astronomical (that's 83-to-1 for 2008, which only improved in 2009 because the number of acquisition deals also fell off a cliff). For those lucky enough to exit by acquisition, the return from a successful acquisition has begun to fall.

Now, you might say that the more than 700 cybersecurity firms already present in the market are simply too many, so why start others? Fair question. But if we look at the publicly traded security firms and pool their R&D budgets, that curve is slowly declining, so the majors are not making up for entrepreneurs' loss of opportunity, nor are the majors keeping up with either the rise in vulnerabilities nor our two indices—and we claim that our indices reflect nothing so much as the investments being made by our opponents. (We do hope that it is our opponent's version of investment rather than our own fumbling that is driving all three.)

However, as Albert Einstein famously said, it's insane to keep doing the same thing in the hope of different results. Maybe investment in cybersecurity, whether tracked by the nourishment of entrepreneurial innovators or by industrial research budgets, is the thing we keep doing in the vain hope of getting different results—you know, cybersecurity will come home if

which is to say the conservative, which is to say the rational—mind seeks approximations that are, at least, correct in their azimuth if not tuned to six-digit precision.

To point the finger at ourselves, our Owned Price and Security Pressure Indices are trend statistics that are as good as our raw material (and honesty) can make them, but which you should read for no more than their direction and relative change in velocity, month over month. Nevertheless, we will (happily) sell you index futures should your appetite for risk be unrequited.

In the meantime, let us assume that cybersec needs innovation and that innovation needs investment. Let us further assume that innovators and investors are different entities who both ignore Buckminster Fuller ("Making money and making sense are mutually exclusive"). What do the numbers—that is to say, the trends—tell us? (Note that all sparklines in the following text have a vertical axis at zero, that is, no tricky truncation of vertical scale for newsworthy effect. Likewise, all horizontal axes run from 2002–2009.)

Using 2002–2009, the numbers tell us that managers of university endowments, pension funds, and other institutional investors are bailing out of venture pools, and, consequently, the average venture fund is quickly getting smaller, a trend even more dramatic when we confine our view to just the size of new funds raised:

This is important; companies that began with venture money today account for 21% of the US GDP and 11% of all domestic jobs. This institutional pullback is clearly an overreaction—world GDP growth ratifies no such dash for the exits.

Closer to home, the need for investment in security innovation remains clear; the curve of newly discovered vulns continues to bend upward, as does our SPI (see the table). Nevertheless, although venture firms continue to devote a fairly steady (~20%) share of their current deal pool to "Internet" companies, venture investment in security firms has fallen by 90% in just five years.

For security innovators making



DANIEL E. GEER JR.
In-Q-Tel



DANIEL G. CONWAY
Augustana College

only we wish hard enough. Maybe the way forward is not just an arms race by metaphor but more like the real thing. If it were the real thing, then history shows that two paths and only two paths lead to victory:

- fight proxy wars instead of exchanging nuclear bombs, and
- force the opposition to bankrupt itself as a matter of honor.

By the first, we mean identifying, as best we can, the apparent sources of attacks, rank-ordering the resulting list, and derouting the worst netblocks. By the second, we mean accepting that exploitable vulnerabilities are found by professionals and have economic value, so our side simply outbids all conceivable competitors; as a starting point, we would open the bidding at 10¢ per vulnerable platform for a 0day remote—that is, US\$65 million for a remote in Internet Explorer. As with banking insurance, where a risk-adjusted fee on each bank’s financial footprint funds depositor’s insurance against any bank’s stupidity, a risk-adjusted fee on each vendor’s platform footprint would fund the pool for cornering the market in vulnerabilities.

As for our regular indices, the ØPI continues to drop, with the current level now \$59,360.20. The index drop results from the decrease in the prices of distributed denial of service (DDoS), stolen bank account information, and passports, which more than offset increases in verified Paypal accounts and email lists. Identities, credit cards, FTP hacks, and RDPs remained basically unchanged. The decrease in passport prices is actually a reflection in success for the good guys, as new technologies have damaged this underground market, and the product’s perceived value has been lowered. As a result, older passports are priced higher than newer passports. On the troubling side, bank account login information has dropped as low as 2% of the balance. The drop in DDoS prices

has been widely presented as an oversupply issue. Other interesting prices not captured in the index include Facebook accounts (\$8/thousand friends), ID lookup software as a service (SaaS) (\$6/lookup), and UPS accounts (\$15).

At the same time, our SPI continues to ramp upward (bad), and now stands at 386:

Index	Previous	Current	Trend
Phishing	834	917	
Spam	281	314	
Workfactor	91	77	
Dataloss	138	236	
Composite SPI	336	386	

Acknowledgments

As ever, thanks to the Anti-Phishing Working Group, Commtouch, the US National Institute of Standards and Technology, and the Open Security Foundation for their thankless collection of data. Thanks to Peter Kuper for the venture numbers unique to this issue.

Daniel E. Geer Jr. is the chief information security officer for In-Q-Tel. He was formerly vice president and chief scientist at Verdasys, and is a past president of the USENIX Association. Contact him at dan@geer.org.

Daniel G. Conway is an associate professor of business administration at Augustana College. He previously served on the faculty at Indiana University and the University of Notre Dame. Contact him at danielconway@augustana.edu.

cn Selected CS articles and columns are also available for free at <http://ComputingNow.computer.org>.

Silver Bullet Security Podcast

In-depth interviews with security gurus. Hosted by Gary McGraw.

www.computer.org/security/podcasts

Sponsored by **SECURITY & PRIVACY** digital