

# Margin of Safety or Speculation?

## Measuring Security Book Value

DAN GEER AND GUNNAR PETERSON



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](mailto:dan@geer.org)



Gunnar Peterson is a Managing Principal, Arctec Group, which provides security and identity architecture consulting, development, and training across the globe. Gunnar consults and trains developers, architects, and security pros in secure coding and architecture. He is a contributing analyst at Securosis, an IANS faculty member, and blogs at <http://1raindrop.typepad.com>.

[gunnar@arctecgroup.net](mailto:gunnar@arctecgroup.net)

The measure of success is not whether you have a tough problem to deal with, but whether it is the same problem you had last year.

—John Foster Dulles

**I**n the stock market, financial institutions that are considered to be well run sell at a premium: their stock price is greater than their tangible book value, the price/book ratio. What is that book value? A simple number that is easy to acquire and understand, book value is the asset's dollar value carried on your balance sheet. Applying book value to IT, what cost did you incur to develop, deploy, and operate your system? That's its book value.

Why would anyone pay more than book value for a bank's assets? Because some banks make higher quality loans and take less risk. Investors deem Wells Fargo and US Bank to be well run: Wells Fargo trades at 1.5x book value and US Bank trades at 2.0x book value. Conversely, banks that are thought to be less well run sell below book value: Citigroup has traded at near half its book value since 2008.

The stock market's premium for Wells Fargo and US Bank and its discount for Citigroup may or may not prove to be well founded, but what those price ratios tell you is the value that investors place on the quality of the assets and the risk management of those companies.

In this spirit, we propose using a Margin of Safety calculation to compare the book value of a company's IT assets (software, servers, development, and so on) to book value of the security controls and services used to defend those assets. We suggest that the difference between these two numbers assesses the level of safety for assets in your enterprise. If the assets' book value is well covered by the book value of the security controls, then you are making minimal assumptions as to the efficacy of your security systems. If the gap is wider, you may be asking for heroic efforts—too much—from your security services and team.

In investing, paying less than \$1 for \$1 of assets is an example of a Margin of Safety. What we seek to show here is where the line between safety and speculation occurs in information security systems.

A disclaimer: we make no attempt here to address a number of important concepts. We consider the basic book value to be a number, a number that has the personality of a brick; it does not change much, it is not subject to interpretation. To us, that's beautiful. It's also limited. In using the book value metric, we do not address the earnings power of the assets, nor do we attempt to measure the efficacy of the security controls.

## Margin of Safety or Speculation

The earnings power of the assets is arguably the single most important business metric; the efficacy of the security control is arguably the most crucial security metric. Why, then, do we propose to not address either? Simple—both earnings power and efficacy are highly subjective, path dependent, fraught with errors, time varying, and prone to willful misinterpretation. You throw out a subjective number in a meeting and then defend that subjectivity to anyone who disagrees. This is metrics at their worst, people marinating in their own biases rather than letting the numbers do the talking.

Book value, on the other hand, is appealing for all its brick-like qualities. For one thing, it is hard to argue with. You either paid \$10M for SAP or you didn't. It's there in black and white, and, better yet, the accounting department will back you up on it.

Okay, so it's a good number, but what can you use it for? To quantify assumptions, illuminate priorities, and identify opportunities for improvement.

To illustrate how book value quantifies assumptions, let's consider a company that runs a customer Web site and a customer mobile app.

The customer Web site cost \$5M to develop and deploy. The company spent \$250k on security software and services for that Web site.

The mobile app cost \$1M to develop and deploy. The company spent \$25k on security software and services for that app.

Now we use the Asset/Security ratio to compare the cost of the project versus the cost of the security services in Table 1.

The Margin of Safety shows that the mobile project has, on a relative basis, invested half as much in security as the Web app. Margin of Safety is a coverage metric. Coverage metrics are useful precisely because of the assumptions they do not make. Applications and systems are built to do something functional. Functionality can be measured in the present. Risk lies in the future. The Margin of Safety cover shows what's invested to absorb unfavorable future events. The Web app team invested 5% of its budget in failure mitigation.

	Web	Mobile
Asset	\$5M	\$1M
Security	\$250k	\$25k
Asset/Security Ratio	20	40
Margin of Safety	5%	2.5%

**Table 1:** Asset/Security ratio for our example Web site and mobile app

Does this mean the Web app is secure and mobile is doomed? Hardly. What it does mean is that company management is assuming one of the following: the mobile security team is twice as effective as the Web team or the mobile threat environment is half as dangerous as the Web threat environment.

Calculating the Margin of Safety for Web versus mobile shows a simple way to compare across projects, that is, the Margin of Safety imposes an ordinal scale across those projects and ordinal scales are decision support tools, per se. The metric is a means to an end, not an end in and of itself. Are the managers who allocated half the security budget to mobile assuming the team can execute? Are they assuming that they have tools to close the gap? Are they assuming "no one hacks mobile"? Looking at book value does not answer these questions, but it gives a framework to ask these questions, and have rational conversations about how to move forward.

Book value can be used for security architecture, not just projects. Consider what your organization spends on network, host, application, and data security, then compare its book value to the book value of the non-security spent to develop, deploy, and operate those assets.

To illustrate, we fabricate Table 2. In it, what we see is that IT assets like applications and data are underinvested. Assuming the developers and DBAs are highly skilled, care deeply about their work, are trained in secure coding and configuration, and have built their own tools, this could be a non-problem, but absent assumptions like those, the Margin of Safety points to a yawning gap in security coverage of the organization's most valuable IT assets.

In short, security spending should be treated like a bank's assets—a purchased good that is on the books. Using that book value as the starting point lets you cleanly separate the objective measure (book value) from the assumptions you are making (leverage ratio). The amount you extend beyond your security spending is your company's leverage. Note that, just as with banks, leverage itself is risky and amplifies any risk that you already have on your books.

	Security	IT Dev & Ops	Margin of
	\$amt/year	\$amt/year	Safety
Network	1,000,000	2,000,000	50%
Host	750,000	3,000,000	25%
Application	350,000	5,000,000	7%
Data	50,000	2,000,000	2.5%

**Table 2:** Some values fabricated to illustrate differences in the Margin of Safety

## Margin of Safety or Speculation

## Margin of Safety benefits:

1. Almost anyone at any level in the organization can calculate this for any of their projects in ~20 minutes.
2. The Margin of Safety can be compared across projects.
3. Gives you a way to see where you are more exposed and some idea where to allocate resources.
4. Uncontroversial and simple to understand metric.

## Margin of Safety limitations:

1. Silent on the quality of either earnings power or efficacy.
2. Silent on threats and deployment—so manually you would need to adjust for what is appropriate “internal” leverage vs. DMZ leverage.
3. Like most everything, datasets are likely not available to the general public to test.

As to the benefits, try it out and report back. As to the limitations, we prefer silence to rank speculation.



## Do you have a USENIX Representative on your university or college campus? If not, USENIX is interested in having one!

The USENIX Campus Rep Program is a network of representatives at campuses around the world who provide Association information to students, and encourage student involvement in USENIX. This is a volunteer program, for which USENIX is always looking for academics to participate. The program is designed for faculty who directly interact with students. We fund one representative from a campus at a time. In return for service as a campus representative, we offer a complimentary membership and other benefits.

A campus rep's responsibilities include:

- Maintaining a library (online and in print) of USENIX publications at your university for student use
- Distributing calls for papers and upcoming event brochures, and re-distributing informational emails from USENIX
- Encouraging students to apply for travel grants to conferences
- Providing students who wish to join USENIX with information and applications
- Helping students to submit research papers to relevant USENIX conferences
- Providing USENIX with feedback and suggestions on how the organization can better serve students

In return for being our “eyes and ears” on campus, the Campus Representative receives access to the members-only areas of the USENIX Web site, free conference registration once a year (after one full year of service as a Campus Representative), and electronic conference proceedings for downloading onto your campus server so that all students, staff, and faculty have access.

To qualify as a campus representative, you must:

- Be full-time faculty or staff at a four year accredited university
- Have been a dues-paying member of USENIX for at least one full year in the past

For more information about our Student Programs, contact Julie Miller, Marketing Communications Manager, [julie@usenix.org](mailto:julie@usenix.org)

[www.usenix.org/students](http://www.usenix.org/students)