Using Benchmarking to Make Better Security Decisions
Transcript

Part 1: What Is Benchmarking and Why Is It Useful?

Julia Allen: Welcome to CERT's Podcast Series: Security for Business Leaders. The CERT program is part of the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org.

Show notes for today's conversation are available at the podcast website.

My name is Julia Allen. I'm a senior researcher at CERT, working on security governance and executive outreach. Today, I'm pleased to welcome back Betsy Nichols, Chief Technology Officer at PlexLogic and a faculty member at the Institute for Applied Network Security. Today we'll be discussing benchmarking and how it can contribute to your information security program. So welcome back, Betsy.

Betsy Nichols: Thanks, happy to be back, and thanks to CERT for inviting me to participate.

Julia Allen: I think this will be a nice follow up to our last podcast. We did talk previously about security metrics. So let's segue into benchmarking. And can you say a little bit about it and how do metrics and benchmarks relate to one another?

Betsy Nichols: Okay, great. Well, I suppose the shortest definition for benchmarking is just to define a point of reference for measurement. So metrics, of course, are all about measurement and benchmarking is all about really making comparisons. One type of comparison is a best practice type comparison, where essentially you're saying, "Here's a definition of perfection," and you're trying to define some measurement as to how far you may deviate from it. Another is more of a normative kind of benchmark, where what you're doing is measuring a group of people and saying "What's typical and am I above or below the mean or in a certain percentile?" So that's one variant. There are other variations on benchmarks that have to do with timing. For example, some people do benchmarking in real time in order to detect anomalies from a norm and take corrective action. Another is a more sort of strategic application where what you're trying to do is find out norms over time and use benchmarks to make better decisions.

Julia Allen: So would it be fair to say then, having a benchmark or a reference point allows me to put my metrics or measures in some type of meaningful context?

Betsy Nichols: Yes, that's perfect.

Julia Allen: Okay. So how are benchmark results typically used? And how might a business leader use benchmarks to help them get on point with their security program?

Betsy Nichols: Well, in talking with a bunch of CISOs (chief information security officers), the sorts of uses that I've seen them describe to me are, number one, to provide hard evidence of a competitive advantage. In many respects, they'd like to be compared to their peers so that they can make the case that they're better than they are. An example would be security budget per employee. That's an interesting benchmark that people could use to demonstrate, I suppose, their commitment to benchmarking, or commitment to security, I should say.

Other uses would be to identify areas that require improvement, where maybe you don't compare so well to your peers. You can defend proposed budget or staff expenditures with benchmarks. Certainly you can drive performance improvement and measure it. You can communicate performance to executives in a very crisp and concise manner that typically is pretty easily understood. The common thread for most of these uses is that a benchmark provides information that will lead to better decisions and that in turn will lead to a better IT security program.

Julia Allen: So if you take this whole notion of putting your measures in context – often we'll see someone reference a best practice and you should do it just because it's a best practice. And yet when you have the benefit of benchmarks, it occurs to me that — say you're in a financial services sector, in the manufacturing sector — you can actually get a much better handle on if that practice is good and useful given the business that you're in. Is that potential there?

Betsy Nichols: I think that's absolutely true. The benchmark does allow one to compare one's performance to one's peers and add context to it that way. I guess the other point I would make is that doing well for the sake of doing well, while that's certainly a valuable context, you also want to know that doing well with a particular benchmark leads to better security, whatever that means. And better security in some contexts may be reflected through benchmarking on security practices that would, let's say, reduce the likelihood of a data loss event, or increase the availability of systems because they're more secure and have a lesser tendency to fail because of security problems.

Julia Allen: It also occurs to me that, we know that you can't secure everything and so you have to make some risk-based decisions about what actions to take. And I would think that benchmarks could help inform, as you said, inform that decision making process.

Betsy Nichols: Absolutely.

Part 2: Benchmarking Challenges and Some "Works In Progress"

Julia Allen: In your experience, and in your work with your clients, what are some of the major roadblocks to security benchmarking?

Betsy Nichols: Well there are several. (1) The first one is just arriving at really crisp, unambiguous definitions of what the benchmark will be. How do you compute it? What precise data is required? What counts? What doesn't count? This can be harder than it may sound.

(2) The second barrier is really having a trusted third party, some dispassionate entity that can be trusted to collect, compute, publish, and protect the benchmark's integrity and confidentiality and accuracy. This means that benchmarking has to sustain itself really as a business. A third party has to be able to stay in business to do this.

(3) And the third one I would mention, third barrier, is what I would call market gravitas. The best way for me to describe this is by analogy really. If you look at other famous benchmarks from other areas outside of IT, benchmarks such as the Nielsen media ratings, or the College Board SATs, or Moody's, as examples, all of these are benchmarks that have what I would call market gravitas. In the case of Nielsen, a good rating maps the ability of a media outlet to charge higher advertising fees. So there's a business reason to allow one's self to be rated. In the case of College Board exams, good SAT scores can map to college admission success for an applicant. In the case of Moody's, higher ratings map to financial benefits. So market gravitas is very important and probably, in my opinion, the most difficult roadblock of the above three anyway to overcome.

Julia Allen: So obviously what you're saying is there needs to be a business case for the benchmark.

Betsy Nichols: Yes. There needs to be a business case and there needs to be enough value in the benchmark to sustain a trusted third party to do it.

Julia Allen: That makes good sense. So obviously benchmarking involves sharing data, right? And some of this data is sensitive. So in your experience, is it possible to conduct meaningful benchmarks without fear of losing privacy or data confidentiality?

Betsy Nichols: Well, this is an interesting question. And I guess what I have to say is the answer is yes and no.

Julia Allen: Okay.

Betsy Nichols: Let me explain that. I would say yes, in terms of protecting the privacy of the individual companies or the business units or the people, let's say, that are being measured. I think that can be done. And I can talk more about that in a minute.

But what I mean by "no" is, it does not necessarily protect the group in terms of publishing characteristics of the group as a whole. And that can have a downside. So let me give you an example. Suppose that we established a benchmark called "account latency." That's really a key performance indicator that measures the mean time, let's say, elapsed, between an employee's termination from a company and the removal of all that employee's IT access to accounts. Say it's in units of hours, for example. That would be our benchmark metric. It would be a way of measuring the relative performance of companies in managing access to sensitive data, let's say. If there were 300, 400 companies involved in a benchmark project, or even more, it would be fairly straightforward, in other words, known art, to protect the transfer and storage of the benchmark metric results from each of the participating companies to the benchmark center. The statistics in determining each company's individual performance and comparing them as peers, that's also known art. It's not particularly difficult statistics. As an example, you could just use percentiles to rate their performance. Moreover, I would say the protection of each company's individual percentile would be relatively easily protected. Certainly it's known art. The companies that did well might even choose to reveal their results. They could say, "Well, we're in the 95th percentile," and they wouldn't be revealing anything else about the other companies.

So the answer is "yes" for the individuals. I think that's not the problem. What is most difficult is protection of the overall state of the peer group. In terms of account latency, let's say, if a company reported that it was in the top five percent of latency but its latency was three days, then that's some information that would be useful to the dark side, so to speak, or the black hats out there.

Julia Allen: Right, because if they know that a particular sector has that kind of a delay between termination and removal of the accounts, then that clearly gives them a window of opportunity.

Betsy Nichols: It absolutely does. And it defines how long they should work at cracking that particular point of vulnerability. So it's interesting. It sort of takes a very special point of view for the peer group to say, "Okay, it's okay for us to let this information come out. It's going to drive improvement. And in the interest of driving improvement, we'll live with it." This is an example, I guess, of a specific benchmark where that risk is particularly acute, or that problem is more acute. There are other types of benchmarks where the problem is probably less acute.

Julia Allen: So building on that notion of the data sensitivity and the upside and the downside, what have you seen as effective approaches for building these trust relationships such that business leaders will actually be willing to share data with one another so that the results can be useful?

Betsy Nichols: Luckily there are a few. And I think there're some that are really making good progress. One example is the ISACs. ISAC stands for the Information Sharing and Analysis Center. These are federally mandated groups and they are organized to serve particular market segments. So for example, there's the FS-ISAC, which serves the financial services sector. And the MS-ISAC, multi-state ISAC, that serves state governments.

To date, these entities have been successfully established as trusted third parties. They have memberships that number in the hundreds, if not thousands. And to date, the primary information that they've been sharing is cyber and physical threat data. If one organization sees a threat, it notifies the central organization, the central ISAC, and then that ISAC takes care of disseminating that information. So it's not really, strictly speaking, benchmarks. But these organizations are actively looking at expanding their services to include benchmarks. And I think they're well positioned, both financially and trust-wise, to serve that purpose.

Julia Allen: So are there some particular mechanisms they've put in place to establish these trust relationships? Or is it more just person-to-person and knowing each other?

Betsy Nichols: Well, of course, the federal mandate doesn't hurt. They are kind of classic associations. They're dot orgs. And they have membership so they charge a membership fee. And I think that probably the initial level of trust was to some degree a by-product of the federal mandate. They also have people from Department of Homeland Security on their Board. There's a lot of participation from the federal government to try to encourage sharing. And then I think their reputation has increased as they've become known and there have been no breaches.

There are some other examples that I could mention, I guess. I mean, one is the Computer Security Institute, CSI. They conduct an annual survey. And there are typically 400 or more companies that fill out the survey. The published results, I think, are universally read by everyone. So it's something that people pay attention to. They do their reporting in a benchmark sort of context by comparing peers. And while the survey sometimes lacks a certain, let's say, rigor in terms of how consistently it's performed year in and year out, and people complain about it, still, I think it's an influential benchmark that exists.

Another one that I wanted to mention was the Center for Internet Security benchmarks, the CIS benchmarks. I mention those really for two reasons. The first is it's a great example of a best practice benchmark, as opposed to a normative benchmark, which is primarily what CSI was doing. The second reason I mention it is that it's been sustained over a long period of time and it's got a record of continuous progress. And I think it's gaining momentum over the years.

Part 3: Keeping Benchmark Data Up to Date and Getting Started

Julia Allen: Well, you've really segued nicely into my next question with the Center for Internet Security example, which is, given that the landscape's always changing, what are some effective ways, in addition to those you've mentioned, to keep benchmark data up to date?

Betsy Nichols: They have a particularly tough problem because their benchmark is extremely technical. It looks at essentially the deviation of a target system from an ideal configuration. And with the changing in technologies, for example, now just with the introduction of Microsoft's Vista operating system, a lot of their benchmarks become, certainly not obsolete because there's a lot of

legacy equipment out there running earlier operating systems. But clearly they have to make changes in order to accommodate those changes in technology. So certainly that's one challenge for benchmarking, is to essentially expand the metrics to reflect the new technologies.

I think the other is as people become more adept at using security technologies, and to some degree eliminating certain risks through the wide deployment of those technologies — virus management comes to mind as one example, certainly firewalls is another example — one has to adjust the sort of curve that you're using to score people. It may be that 90% coverage of virus was good once but it certainly isn't good now.

Julia Allen: And it also occurs to me in terms of keeping benchmark data up to date – when you mentioned the Nielsen's rating example and the Moody's example – if you do have a market pull where people are actually using the data actively and want to keep comparing themselves to it for some business-driven reasons, that kind of creates a natural market incentive to keep the benchmark data fresh.

Betsy Nichols: It's very interesting. I mean, with respect to the Nielsen, I would like to mention that recently they've made all kinds of changes in the way they do their measurement to accommodate the college audience. It used to be that colleges and universities, their viewing was never measured. And now it's viewed as a significant market segment that was under-addressed before that they had to deal with.

Julia Allen: So given all this great insight that you've provided for us and some really kind of meaty issues to think about, what are some good first steps that you've seen or that you've participated in for getting a benchmarking program started?

Betsy Nichols: Well, I think clearly the best place to start is with really an internal benchmarking program that is really an adjunct to a metrics program. Here what you can do is you can compare various entities within the organization. You could compare one business unit against another, you can compare one technology against another technology. So there are many opportunities to begin doing benchmarking just internally. And it has, obviously, two advantages. One is that a company just can unilaterally decide to get started without the need for a broader mandate from its peers. The second advantage is that a company can identify useful benchmarks within the privacy of its own IT operation and then bring that to the table once a peer, perhaps a peer benchmarking effort gets under way.

Julia Allen: One of the other things that I've seen is it can also stimulate some friendly competition, right?

Betsy Nichols: Yes, absolutely. That's been mentioned as one of the major benefits for just about everybody I know that has a metrics project that incorporates some benchmarking.

Julia Allen: Well Betsy, this has been great, and I think very insightful and actually a nice way to frame some real concrete actions that organizations can take and get some positive benefit from, so I sure do appreciate your time and look forward to another future conversation.

Betsy Nichols: Terrific. Well, I've enjoyed it. Thank you.