Initiating a Security Metrics Program: Key Points to Consider
Transcript

Part 1: Using Metrics to Make Better Management Decisions

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 web site.

My name is Julia Allen. I'm a senior researcher at CERT working on security governance and executive outreach. Today I'm pleased to introduce Sam Merrell, a member of CERT's Survivable Enterprise Management Team. Today we'll be discussing topics to consider when developing an information security metrics program. So welcome, Sam, glad to have you with us today.

Sam Merrell: Thank you Julia.

Julia Allen: So I understand that you are specifically investigating security metrics as they relate to the U.S. Government's Federal Information Security Management Act, often known as FISMA. Can you tell us a little bit about this work?

Sam Merrell: Yeah, sure. The Survivable Enterprise Management team is, as you said, a part of the CERT Program. And part of our work is to help implement strategies for managing security improvement. So part of that work involves cooperation with U.S. federal civilian agencies who are all bound to the FISMA regulations. FISMA itself establishes a framework for improving the management of information security controls.

So this need to manage and improve controls implies that we need to have a comprehensive measurement program in place. So what we do is we try to work with organizations not only, as I said, to improve their management, but also to develop metrics and measurements to allow them to make better management decisions.

Julia Allen: So obviously, FISMA establishes regulations for federal government agencies and as you said, from these regulations and requirements come controls. And am I correct in saying that the only way you really know if you've been successful in putting a control in place is to have some way to track, measure and report on it?

Sam Merrell: Yeah. Normally people bring out the adage, "What gets measured gets managed," or "What gets measured gets done," something along those lines. That's the conventional wisdom, I guess.

Julia Allen: Sure, because if you aren't watching what's going on you really don't have any idea if what you've put in place is really effective, right?

Sam Merrell: Right, or whether or not you can make any improvements.

Julia Allen: So let's take that a step further. In your experience, how do metrics contribute to building and sustaining an information security program?

Sam Merrell: Well, they serve as the foundation for feeding management decisions whether they're about resource allocations, and budget, and time, or personnel, or by implementing different controls or better controls. A measurements program or a metrics program will allow an organization to understand how it's meeting its security objectives.

Julia Allen: In our governance work we talk about this issue of decision making, and from what you've said, metrics as a basis for well-informed decisions. That's really the tough part about security. There's so many things that need to be done, and is it correct that metrics can really help you get a handle on what the most important things are to do?

Sam Merrell: They can. They can provide a way for an organization to understand how it's meeting strategic goals and objectives, things that have been explicitly stated within organizational plans such as strategic planning, or even some tactical documents, to let you know how well you're accomplishing the goals that you decided were important to the organization.

Julia Allen: So how would I know a good metric if I saw one in contrast to a bad one? What are some of the characteristics of the metrics that you recommend?

Sam Merrell: Well, actually there's a book by Andrew Jaquith who has a lot of advice on this. It's called Security Metrics [: Replacing Fear, Uncertainty, and Doubt]. And he says basically a good metric is something: (1) that's consistently measured without any subjective criteria; (2) something that's easily gathered; (3) that's expressed as a number or a percentage; (4) and expressed at least using one unit of measure such as hours or dollars; (5) and is very relevant to the stakeholders or the people that will be consuming the metrics information.

Bad measurements come from, I guess you could say, unstable programs or things that aren't measured reliably at every time. What NIST recommends is an entire metrics program that outlines explicitly: (1) how you're going to go about collecting information; (2) what information you're going to be collecting; (3) how it's relevant to the stakeholders; (4) how you're going to be analyzing it; (5) and how you're going to be reporting it.

Julia Allen: I know that NIST, the National Institute of Standards and Technology, has a key role in defining guidelines to help U.S. federal agencies comply with the FISMA regulation. What are some examples of effective security metrics that NIST has defined to help meet those compliance requirements?

Sam Merrell: Well NIST has issued a number of documents now to guide agencies on how to implement and manage security metrics programs. However, only one is actually part of the NIST official publications. The other two are right now in draft. Special Publication 800-55 is the one that's currently available and that's Information Security Metrics Development [Security Metrics Guide for Information Technology Systems]. That shows an organization how to go about establishing their metrics program, involving stakeholders, and evolving your metrics program to understand where you are as far as almost a maturity level – to understand how to gage your implementation of information security controls and then manage improvement of those controls over time.

Julia Allen: And you mentioned that there are two others in draft?

Sam Merrell: There are. 800-80 [Draft Guide for Developing Performance Metrics for Information Security] was one that came out, I think it was about a year ago or so. And actually the folks at NIST have asked that I tell people that although it's in draft, it's not actually going to be released at any time because that's been superseded by a revision of the original 800-55.

What NIST has done over the last number of years is they themselves have evolved from what started out to be a very system-level approach, looking at the box itself to manage information technology, and they expanded that to an enterprise approach — sort of along the lines of what we do here at CERT — taking a look at the macro level, or the organizational management of information security, realizing that the information extends beyond the computer itself that it might reside on.

Julia Allen: So you're saying that in some of their guidelines they really moved from more of a computer, or network, or IT orientation to more of an information and enterprise orientation.

Sam Merrell: Exactly. Their philosophy's expanding beyond the technology of the system and into the enterprise use of the system, or the actual information is probably the better way to put it.

Part 2: Challenges and First Steps

Julia Allen: Oh, that's a good point. So, Sam, again in your experience and in your work with your clients and customers, what do you find are some of the difficulties that organizations have in developing and managing a security metrics program? Why is it so hard?

Sam Merrell: Well, first, as I said, a good metrics program has to be rooted in stable repeatable processes, and that's probably one of the biggest obstacles. It's very important for organizations to have policies and procedures that they know where to measure reliable points over time. So you need to identify your data source and know that it's going to be there the next time you need it. That's probably the biggest obstacle. A lot of times processes are ad hoc that can't be repeated very successfully, so organizations struggle whenever they need to actually measure, or at least re-identify what points they need to measure.

Also organizations tend to struggle with involving all relevant stakeholders. A lot of times people will identify at the wrong level in the organization what should be measured, and then try to feed that information either up- or downstream, only to discover after putting in a lot of work and trying to measure these processes that the information generated isn't very relevant to the consumers. So those are two very, I guess, common barriers that organizations will face.

Julia Allen: Based on my reading and research it just seems sometimes it's hard to figure out what to measure that is meaningful, going back to your comments about decision making, what really helps inform the decision making process, right?

Sam Merrell: Right. Like I said, the NIST approach is a useful one. If you start by looking at the strategic drivers of the organization, and then break that down into understanding what are those, what we call the critical success factors that allow those to happen. Try to dissolve the strategic statements into very tactical daily operations which then you can see what's important to the organization, and drive your measurements or your metrics needs from that point.

Julia Allen: So if you were going to help a customer get started, what would you encourage them to do say, first, second, third in putting their metrics program in place?

Sam Merrell: First take a look at their processes. Make sure they have repeatable processes, that they understand what their strategic goals are, and understand what's important to them. Second, make sure they understand their security objectives so they can really make those sound management decisions understanding what's important and critical for the organization to

measure. And then involve all stakeholders in the creation of metrics requirements so they understand and have a very deep knowledge of who should be consuming what information.

Julia Allen: Have you seen any instances of, thinking back to this difficulty with decision making and coming up with the right metrics, have you seen any instances where organizations have taken their security metrics, or their desire to have security metrics, and tied those into other measurement processes in the organization? Say, going back to Andrew Jaquith's, or going back to Balanced Scorecard, or quad charts, or heat graphs, or other ways of taking the security state and actually reflecting it within the broader context of other enterprise measurement approaches.

Sam Merrell: Well, I think organizations generally face a sort of a challenge. This approach of trying to generate your own metrics means that whatever organization A elects as their own performance metrics will be different than whatever organization B is. So whenever you come to well known tools such as dashboards, and things like that, there's a challenge because a lot of the vendors and the people who create these dashboards want to create metrics that will work across organizations. So these tools that gather this information don't necessarily have the broad applicability across organizations to be able to be applied whenever we're saying "build your own metric, generate your own information." So you don't really have that roll out capability, or at least I haven't seen it.

Julia Allen: Okay. So it's kind of one of those things maybe take a look at but buyer beware.

Sam Merrell: Exactly. Just be informed may be a better way to put it.

Julia Allen: Well, Sam, this has been really helpful to kind of get the stage started on talking about security metrics, and we'll certainly link to your Federal Information Assurance Conference presentation in our show notes which has a lot more detail. Is there anything else in closing that you'd like to pass along to our listeners?

Sam Merrell: Well, there's some great resources out there. There are a couple of public web sites that are available. Actually our own CMMI has some very practical guidance within the measurements and analysis process area on how to get started on a very sneaker-wear type level. You can actually take action on it. We've seen a couple of commercial enterprises out there. Elizabeth Nichols has done some really interesting work in this area. And then the NIST guidance itself has some really great information. Good luck.

Julia Allen: Well, thanks a lot.

Sam Merrell: Thank you.

Julia Allen: And appreciate your time.

Sam Merrell: Excellent. Thank you.