Title: Getting to a Useful Set of Security Metrics
Transcript

Part 1: Metrics as a Means for Directing Attention and Energy

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 software assurance. Today I'm pleased to welcome back Clint Kreitner, the president and CEO of the Center for Internet Security. We'll be discussing the challenges in creating a common set of widely accepted security metrics that security professionals and business leaders can use to make better informed decisions. So welcome back Clint, glad to have you with us today.

Clint Kreitner: Thank you Julia, my pleasure.

Julia Allen: So as a business leader you've assumed many roles in your career. Could you please share some of the ways you've used metrics?

Clint Kreitner: I'm a great believer Julia in the use of metrics as a leadership resource to direct the efforts and energies of an organization. When you think about it, we human beings are information driven entities, all the way from the cellular level in terms of the way our immune system works, all the way to how we behave at a basketball game or a football game. We react to the numbers that are on the scoreboard in certain ways and so on.

But particularly in my experience as a hospital leader, we were able to use metrics as a way of focusing the staff on things that were important, and also as a way of getting them out of their individual silos. At one hospital I worked at we put an IBM PC – this is in the early days of the IBM PC – in the cafeteria where staff members could go and take a look at our financial status, our patient satisfaction scores, our infection control statistics, and that sort of thing. And it had a very revolutionary impact on the staff, causing people to ask questions about how what they did impacted our financial performance or our ability to prevent hospital-acquired infections and so on.

So I've just seen it over and over that if you, as a leader, if you craft a few pointed metrics, if you will, that deal with the – fundamentals of the business, of the enterprise, and post them very visibly, people will look at them, people will understand them – or if they don't, they'll ask questions and it provides a wonderful opportunity for learning.

And so I'm just a great believer in posting scores on how we're doing, in all the key areas, and then letting people digest that information and relate it to the work that they do and how it contributes, how their work contributes to the overall success of the enterprise.

Julia Allen: Well as you said starting out, we're information driven and we're also suffering from incredible information overload. So certainly my experience matches yours in that metrics really helps you kind of focus your attention and your energy, and help you decide where to take action, correct?

Clint Kreitner: That's an excellent point Julia, and it applies in spades to information security. Because information security, like safety, is one of those areas where there's perhaps an infinite

number of things you can think of to do that would improve security, but how in the world do you decide which ones to invest in first, and then which ones to invest in second and so on?

So yes, the tremendous volume of information that's thrown at us these days needs to be winnowed down to some key metrics. And interestingly, the finance folks have done this for probably centuries. We all know how to read financial statements, and financial statements are full of financial metrics. And so we need to do the same thing in other areas of enterprise life.

Julia Allen: So Clint why does there seem to be – kind of honing this into our subject at hand – why does there seem to be a growing interest in information security metrics in particular?

Clint Kreitner: Well I think there's a couple of major reasons Julia, and then some supporting forces and pressures. The two main ones I think are first of all pressure from management being applied to the information security professionals, saying "Justify the money you're asking us to spend on protecting information." And secondly, the current inability of the information security professionals to respond to those managers with a convincing case.

So far, if we're really honest with ourselves, when it comes to information security investment, we pretty much throw everything we can at the problem and hope for the best. We have very little idea of which practices are more cost-effective in terms of money spent versus protection provided.

The second reason, the second major reason I think is growing pressure, resulting from these personal information disclosure laws that are now in effect in – I don't know how many states, but 30, somewhere between 30 and 40 I think. Enterprise leaders read the paper and they hear story after story after story of stolen laptops and compromised PDAs and breaches involving the disclosure of personal information. So they're beginning to get the picture that this is a problem that's not going to go away and that they're likely to be hit. And when they are, they need to have some reasonable explanations to the regulators, or to the judge, if they are involved – find themselves involved in a legal suit – they need to be able to say something intelligent about what they're doing, or what they were doing to provide what the courts are beginning to talk about as "reasonable security."

So they realize that metrics are a huge value in making a case, that we're doing the right things. We're going to have incidents, we're going to have breaches, we're going to have embarrassments, and we need to figure out – just like with any other aspect of business such as employee safety, for example, in the manufacturing setting – how to spend our money intelligently, and metrics will help us do that.

Part 2: Some Challenges, and Work in Progress

Julia Allen: Well I think we're both aware of a lot of activity in this area. So it isn't through lack of earnest effort to try and come up with some kind of common set of widely accepted metrics. So why do you think we're having such a tough time making progress?

Clint Kreitner: Well I can think of a couple of reasons. One is that the scope, the magnitude of the information protection challenge is, I believe, unprecedented in human experience. The fact that we are so interconnected on this planet that information can flow in the blink of an eye from one side of the planet to the other, and that huge amounts of valuable information can be stored on a device that is very small, physically small, and very subject to theft or loss, is daunting to people – and rightfully so.

But at a more granular level there is a huge problem, I think, within the scope of an enterprise because the people that are involved at the board level in enterprise governance, and the people who are involved down in the trenches as system administrators trying to configure their systems and keep people from – keep people's hands out of the them so that they don't change things – are a world apart in terms of their conceptual frameworks and their language.

And to exacerbate that I think that a lot of security professionals could do a lot to understand more thoroughly, or learn better, how to talk about security in business terms; to realize that security is either a business enabler or it's a disabler – the same as safety, the same as product quality, the same as customer service. Those are all business enablers or disablers. And so the security folks have got to stop thinking about security as an end in itself and they need to think about it in conventional business terms – product quality, customer satisfaction, customer trust, profit, etc.

Julia Allen: Well that's a nice segue into the next question, because while we talk about this daunting challenge and getting our heads and hands around the problem, there has been some great work done in this area. So it would be helpful if you could kind of mention and summarize some of the key initiatives that you're aware of.

Clint Kreitner: There has been some good work done Julia, and much of it has not gained much traction. Back in 2003, one of the subcommittees of Congress convened a group called the Corporate Information Security Work Group, which you are aware of because you were involved with it, where a number of, a sizable number of very bright people were challenged by Congressman Adam Putnam to come up with an inventory of best practices and an inventory of metrics that enterprises could use to improve their management of information protection. It is a set of, as I recall, 99 metrics, divided into governance metrics, management metrics, and technology metrics, that are a good starting point to think about some practical, down to earth metrics that can be used in an enterprise setting.

NIST, the National Institute of Standards and Technology, also has done some metrics work. They have a couple of their 800-series special publications on metrics and how to build them and so on. There is a website, securitymetrics.org, that reflects the leadership of a fellow named Andy Jaquith, who has written a book entitled *Security Metrics*, and a number of other people in the field who have been – a lot of whom are academicians, some of whom are enterprise practitioners, but they have been thinking about security metrics for quite some time. And so I urge you to take a look at some of their work.

And then lastly, I would mention that a project was launched by CIS, the Center for Internet Security, just in the last couple of months, to build upon the work of all these others that I've mentioned – to reach consensus on initially just a few security metrics that we think would be useful and also measurable, practically – capable of practical implementation in the enterprise setting. This effort has two components: one is to reach consensus on a small number of metrics; and then secondly, we're building a database infrastructure whereby enterprise users of these metrics will be able to submit their values to the database. And as the database builds in volume of data submitted, the distribution curves – that'll enable the development of distribution curves, so that the participants who've been submitting their data will be able to compare their data with the distribution curves, comprised of data from other organizations, so they can see where they stand relative to others; which is a strong felt need in many enterprises.

So we're really excited about this project. When it includes information on metrics having to do with security breaches or incidents, and when it has information on metrics relating to the use of certain security practices, then we'll be able to begin to correlate the use of certain practices with a reduction in the frequency and the impact of security breaches, for example.

Part 3: Where to Start

Clint Kreitner: An honest assessment of what we're doing in security these days is that we don't know which of the practices that we are implementing are helping, or to what degree they're helping, or whether they're cost effective from the standpoint of how much it costs to put those practices in place.

Julia Allen: Right, so yes one of my frustrations has been as a community is that we keep producing more and more lists of practices, more and more checklists, more and more controls, things that we recommend people do, without giving them any ability to select the ones that are most meaningful for the outcomes they're trying to achieve, right?

Clint Kreitner: Right. So one of my very favorite outcome metrics is the percent of breaches that were discovered by internal controls. When you think about it, that metric says we're going to have breaches and some are going to be discovered by outsiders, by hackers, by illicit attempts to penetrate our systems. Some are going to be discovered by our customers, by our business partners, etcetera. But if we could raise the percentage of breaches that are discovered by our internal controls, what does that tell us? That tells us our internal controls are working, right?

Julia Allen: Right, but as you said the key point is correlating those to the internal controls with the occurrence or the lack of occurrence of a breach, correct?

Clint Kreitner: That's correct, yes, absolutely. Well we're assuming – I'm assuming that everybody is tracking breaches these days – I know that to be a fact. They're tracking breaches, they're characterizing, categorizing the breaches by what the cause was or what enabled the breach. And so as we correlate those breaches with what enabled them, we can begin to – there's a learning, a feedback learning there, a causality-oriented feedback that results in learning, and hopefully the learning results in improved practice.

Julia Allen: So are there specific metrics that you would recommend for a business leader who is either starting up a program or wants to augment their current security metrics program? Are there any particular ones that come to mind?

Clint Kreitner: Well yes, as I said before, I really believe that they need to have, all the way from the board level on down, they need to have insight into the security incidents that are occurring. So they need to have some metrics around the frequency and damage of security incidents.

They also should have some metrics surrounding their recovery performance, their incident recovery performance, because incidents do create disruption and it takes time to recover from them.

And then lastly, they should have some metrics which measure the extent of use, or the extent of application or implementation, of some security practices that are known to be effective, such as up-to-date patching, such as the use of, the deployment of standard software images, and such as standard configuration policies and so on. So that over time they can see as they – as more and more and more of their systems are monitored for up-to-date patching and configuration compliance, they can see some impact on the breaches – not only the frequency of breaches but the damage of the ones that are occurring, that they're experiencing.

Julia Allen: Well Clint, you've mentioned just a wealth of sources and information, background, and current activities. Do you have any others you'd like to suggest where our listeners can learn more?

Clint Kreitner: There is one more Julia. The IT Performance Institute has been doing, and continues to do, research as it relates to what we're talking about, and I would encourage people to go to their website. They have attracted – I think it's 300-and-some organizations, and arranged them in high performing, medium performing and low performing IT organizations that have begun to understand what it is that characterizes high performing organizations – that are defined in terms of long mean times between incidents, and short mean times to fix, and low levels of unplanned firefighting work, and high ratios of systems to system administrators and so on. And they're learning that disciplined change management and disciplined configuration management are definitely predictors of a stable and secure computing environment. So they're doing some fine work and I would encourage people to take a look at that.

Julia Allen: Well Clint I really so appreciate the opportunity to discuss this important subject with you today, and also wanted to add my thanks to many others of the work that you and the Center for Internet Security have done to raise the playing field and the level of practice in our community. So thank you very much.

Clint Kreitner: Thank you Julia.