A Workshop on Measuring What Matters
Transcript

Part 1: Purpose; GQIM Process; Workshop Structure

Julia Allen: Welcome to CERT's Podcast Series: Security for Business Leaders. The CERT Division is part of the Software Engineering Institute. We are 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 principal researcher at CERT working on operational resilience. I am very pleased today to welcome three of my colleagues, Lisa Young, Katie Stewart, and Michelle Valdez. We are all members of CERT's Cyber Resilience Management team. And the four of us have spent this past year together developing a one-day workshop, which we call "Measuring What Matters." And that's what we're going to be talking about today -- the workshop, its purpose.

We actually had a chance to teach it for the first time last November at the ISACA Information Security Risk Management Conference in Las Vegas. And we'll be telling you about what our plans are for the next steps for the workshop.

So with no further ado, let me introduce my colleagues. Welcome back to the podcast series, Lisa.

Lisa Young: Thank you, Julia, I'm happy to be here.

Julia Allen: And Katie, really glad to have you with us today.

Katie Stewart: Yep, it's great to be here.

Julia Allen: And Michelle, really looking forward to our discussion. Thanks for your participation.

Michelle Valdez: Thank you so much, Julia.

Julia Allen: All right, so let's start with Lisa, who was our fearless leader for this effort. So Lisa, as our leader, could you start us off by describing what we were up to, the primary purpose, and the objectives for the Workshop?

Lisa Young: Yes, absolutely. So, thank you very much. So, as Julia said, we debuted this workshop at the ISACA Information Security and Risk Management (Conference). So when you think about operational risk management, the reason why we measure things is to make decisions, better-informed decisions, take the appropriate actions for managing risk, and then changing the behaviors and culture at our organizations.

But how do organizations, senior leaders, and managers figure out what the right things are to measure? The purpose of this workshop was to take a strategic approach and understand what operational metrics could be used to make sure that organizations are managing risk in the appropriate manner.

Julia Allen: So Lisa, I know we had a couple learning objectives as we were laying this out and defining what the students would take away. Could you say a little bit about- - maybe about some of the specific learning objectives?

Lisa Young: Sure. The purpose of this workshop was to make sure that we could teach people a measurement approach that was tied to their strategic or business objectives, and for this approach, we asked people to come to the workshop with a business objective from which metrics, specific metrics, would be derived.

So Julia, would you like to say more about the structured approach that we took to connecting real-world business objectives with operational metrics?

Julia Allen: Great. So, for our listeners, normally I'm the moderator, but in this particular case I actually worked with my colleagues on developing the workshop, so that's why Lisa's asking me this question.

So we used a method called Goal- Question-Indicator Metric. And if any of you are familiar with our resilience measurement research, which has been going on since 2010, this is one of the foundational approaches. It was based on early work done by two gentlemen, Vic Basili and Dieter Rombach, applied to software engineering.

And then our own Process Program at the Software Engineering Institute added to that as we worked on things like the Capability Maturity Model and then Capability Maturity Model Integration, and actually added the “I,” the Indicator, in the GQIM acronym.

And then since 2010, we've been applying this same method to operational resilience based on the CERT Resilience Management Model. And the whole idea, as Lisa said, is to start with a business objective. So often we have metrics in our organization that are operationally derived and they don't really tie back to anything that's real meaningful to the business.

So the key question for this method is not necessarily, "What metrics should I use?" but "What do I want to know or learn?" And in our conversation today we'll be giving you more information. But the G in the GQIM process is Goal. So we take a business objective and from that derive one or more goals, the meeting of which would allow that objective to be met. And then the Q is Question.

So then we next develop a series of questions that when answered help determine the extent to which any given goal is met. Questions are really key to this approach. And then once we have some goals and questions, we look for indicators, which are the actual data -- "What data do I need to answer the question, to demonstrate the extent to which I'm achieving the goal?"

And then certainly last, but not least, and sometimes one of the tougher parts of this whole process, is to identify one or more metrics that use the data, a.k.a. indicators, and actually formulate a representation of the data that will make sense, be meaningful to business leaders, to inform the achievement of goals and objectives.

Julia Allen: So, Katie, time to give you some airtime and then we'll get to Michelle. Can you tell our listeners a little bit about how we organized the workshop? It was a very hands-on type of instructional event, so say a little bit about how we put it all together.

Katie Stewart: Okay, sure. So the workshop in Las Vegas was a day-long workshop. We tried to really get the participants to interact both with us and with one another. The first part of the

discussion was more of a lecture format, where we gave background and set the context for the business needs for using a process like GQIM for developing a measurement approach. Where we did have quite a few slides and topics to discuss, we got really good interaction with the participants. They brought up some challenges that they face in their organization for implementing measurement and gave us some ideas that we had not heard before on how to overcome those.

The second part of the workshop really focused on breaking down the process using a couple different examples. We went through a very simplistic example that I know Michelle can talk more about, and we also applied it as a group against a more security-focused example that was a bit more applicable to the folks in the room.

Then the balance of the workshop was spent in group work. We had probably a dozen or so tables with four to five participants. And they were able to actually walk through the GQIM process using their peers for discussion and help to develop the metrics in the end.

As I think Lisa said, we asked them to bring a business objective to work through, and so the workshop really was about working with their team to walk through the process and develop a method that they could take back and implement in their home organization.

We wrapped up the workshop just setting the context again and refreshed some of the concepts that we talked about in the introduction. And we sent the participants home armed with quite a lot of material so that they could take this back to their organization regardless of where they were with the development of their measurement program currently. So that's an overview.

Part 2: Scenarios; Business Objectives

Julia Allen: Great, Katie, thank you very much. That helps put a structure together, and we'll suggest some references at the end that helps fill in some of the details that Katie and Lisa have talked about.

So Michelle, last but not least, it's your turn. One of the things you led for our development were our scenarios. So we did develop several key scenarios that we wanted to use to demonstrate how the method is applied, or the process is applied, before we actually turned the tables loose to work on their own objectives. So could you tell our listeners a little bit about the scenarios that we picked?

Michelle Valdez: Absolutely. We wanted to start initially with a scenario that was applicable to anybody and everybody in the room regardless of their background, and it was focused on brushing your teeth. And we used this to really break down the process and demonstrate it in a way that everybody can easily relate to, whether it's how they brush their teeth or how their kids brush their teeth or how they did as kids.

In addition, we wanted to provide a real-life example of an incident that had occurred at a company in the recent past. And since it seems that every day we have new stories that are hitting the news about cybersecurity incidents, we used one that had gained a lot of attention with Forbes.

And we put together a timeline of what occurred and then used that to then demonstrate how somebody who was working at Forbes could take that incident and apply the GQIM method to

help them to recover and ensure that something like that doesn't happen again by ensuring that they're measuring the right things based on lessons learned.

And then finally we had a general incident management (scenario), so that it was also applicable to the majority of the people in the room, and gave them lots of different examples of how to break down each of the steps, and some actual materials where we did the analysis for them so they could use that as examples both in the workshop and when they got back to their home organizations.

Julia Allen: Great, great. And I know as one of our future plans, I'm scooping my question to you on that, but we're planning to add some additional scenarios, right?

Michelle Valdez: Absolutely. We have two additional scenarios that we're looking at, both to keep our scenarios current and fresh, as we have these ever-evolving incidents that are occurring, but also to have scenarios that look beyond just the cybersecurity but look at other general risk management concerns as well.

Julia Allen: Great. So while you have the airspace, Michelle, let me ask you, and then you and Katie can discuss this together. So this idea of working based on business objectives- - and again, we asked each of the participants to bring some objectives with them or provide them to us in advance as pre-work.

So this was the part that got a little challenging for us, I know, but can you describe how we use both the objectives that they brought and some that we had worked on in advance to get to a meaningful set of topics for the smaller working groups? So why don't you start, and then Katie can chime in.

Michelle Valdez: Absolutely. The advantage of doing this in a workshop at a conference was we had the ability to reach out as part of the prep materials and ask for them to provide in advance their objectives so that we could then as a team look at how to break those down into the GQIM methodology to better enhance their learning while they were at the workshop.

But since you never know if people will respond or not, we did come up with five specific topics that we thought “There could be people that would be interested in walking through it,” if they either didn't have objectives themselves that they brought or that their objectives that they did bring would align with, because they were pretty broad categories.

Once we received the inputs -- and we actually, about half of the participants, surprisingly, did send us their inputs, which was really beneficial because it highlighted the fact that business objectives are not easy to start with, without any sort of background on what exactly we're looking for.

So we were able to increase our time spent on describing what a good business objective is. But it also allowed us to do some alignment, to make sure that we had the right kind of topics that people who were in attendance would be interested in.

And though we didn't do full GQIM analysis on all of the different ones that we received, we were able to align many of them into groups that we had already done, and then also provide some examples that people could use during the workshops if they didn't have one at all to use.

Julia Allen: Great. So Katie, why don't you share with our listeners the topics that we actually ended up picking and maybe a sentence or two about those?

Katie Stewart: Okay. So, like Michelle said, we had five of our own, and then we provided a sixth category for folks to go into if they wanted to work something fictional, actually. The first one was “protecting customer information.” This actually was a heavy hitter. We had a lot of people that were interested in this topic and it was our largest group of the day.

Our second topic was “keeping software assets up to date.” Our third was “user awareness of cybersecurity threats.” This one we went back and forth on as a group whether or not to include prior to the workshop because it was a more -- it was a softer goal, right? It had more of a people focus, training and awareness. But again, this was actually one of our highest- interest topics once we got to the workshop.

The fourth was “reliance on external parties,” and the fifth was “mitigating the risk of disruptive events and incidents.” This one we added late in the game after we started to get responses that fell into this category. This was one that we as a group didn't come up with on our own but a lot of the participants expressed interest in risk mitigation.

The final, which was kind of a catchall category that we talked about, was -- we called it the Forbes case study. As prep for the workshop, we developed the Forbes case study as background and reading for the participants, so say they were a consultant to a variety of different organizations, or this wasn't exactly their job, we offered them the Forbes scenarios as a way for them to work through the process without choosing one of the other five topics.

Part 3: Workshop Insights; Future Plans

Julia Allen: Great, great, Katie. Thanks so much.

So Lisa, let's get you back into the conversation and I'll chime in a little bit. So, this is -- I don't have much structure for this part of our conversation, but can you talk about your experience and the experience of the team as the participants broke into small groups around each of the topics that Katie and Michelle just described.

How did they do? Where did they struggle? Where were they making good progress? What were the different experiences at each table? So as best as you can recall, what did you see happening in the room after we let them loose?

Lisa Young: Well, I think the main thing is that many of the -- so as I believe Michelle or Katie said -- coming up with a business objective, sometimes the person in the audience didn't always have or know what the business objectives were.

So we spent a little bit of time on helping them uncover the business objective and why it was important to their program, to their risk management and security program. But what they started to do I think after we had several discussions is to try to figure out the current metrics that they had, and what business objectives the current metrics that they had were supporting.

And this was important because it sort of gave them an aha moment to say, "Oh, well maybe I'm measuring something that costs money to measure and that takes time to measure, but maybe it's not that important, either to me or to my management."

So I thought going through the process of this, pulling apart the goals, the questions, the indicators and the metrics, helped them see the value in their current metrics as well as understand why the tie to the business objective was so important.

Julia Allen: Yeah. So one of my observations, as you said, objective was tough but -- it always surprises me. I've been working in the measurement space for a long time. It always surprises me that folks start with, "Well, let's just measure," and sometimes the measurement books and the guidelines and practices say, "Well, at least just start measuring something."

But if you can't tie it to something that's meaningful to the business, to a particular critical service or product, to a mission objective, to something that the organization really cares about, it's not surprising that it's hard to get anybody very -- at a senior level of management, in particular those that provide the funding for the measurement program -- hard to get them very excited about it.

And you think about financial measurement in an organization and how based that is in accounting principles and techniques and how critical it is to the operation of the business, and we're all trying to get cybersecurity on the same page, and I think everybody in the room found themselves at various points along that spectrum.

So Michelle or Katie, your experiences from interacting with folks in the room? Anything you'd like to share?

Michelle Valdez: I was just so pleased to see how engaged everybody was. I mean, you could tell from the very beginning of the workshop -- but definitely in the second half when we were working at table, within the tables -- that this is obviously a problem that they're really struggling with.

And having the opportunity to sit at a table with people who are looking at similar business objectives and really kind of problem-solve together what a good way to move through the process would be -- I thought it was, I learned just as much as I think anybody in the room did, walking around and talking to the groups, because they were so engaged. And you could tell that this was an area that they were very particularly interested in.

Julia Allen: Great, and then Katie, any aha moments for you or observations that you'd like to share?

Katie Stewart: Yeah. So, in the beginning, even before the workshop started, I had a few requests from people at different tables to provide examples of good measures. They kept asking, "What are some good measures I can put into my organization?"

But by the end of the session, that wasn't the question that people were asking. They were asking things like, "How do I relate what I'm measuring now to a business objective? Do I still even need to be measuring it? Should I be throwing it out?" So I think we did a good job in the workshop reorienting their thinking from "What should I measure?" to "How do I measure progress against my business objective?"

The second thing I'd add is that we really helped some of the people who are responsible for monitoring day-to-day performance. We really armed them with the tools to communicate with their upper management on their measures, why they're effective or why they're not effective, and really how to help drive that conversation to drive action within their organization against what they're measuring.

Julia Allen: Great, great, thank you. So Michelle, as we come to our close, clearly we had this experience, we got lots of good feedback from our participants, and you are leading the charge for our team for moving this body of work forward. So as you talk about our next steps, maybe you could also highlight some of the participant feedback that has driven those next steps and talk a little bit about where we're headed with this content.

Michelle Valdez: Absolutely. As I was mentioning, I think that we all walked away from this understanding that this is an area that there would be a lot of demand for people to get the opportunity to learn more about.

So we've decided to make this and add this to our public course offerings, because we think that there's a lot of opportunity to develop this material to benefit the community writ large and get training out to those people in industry, academia, and the government who are really struggling with this problem.

There are a few changes that we are making from the workshop based on feedback, both positive and opportunities for improvement from the workshop, to include -- we think that, just based on the pre-work that we got and the conversations and engagement that we had within the workshop, that spending a little bit more time on how to take existing business objectives and make them specific enough that you could actually then use the GQIM method and effectively be able to come up with what to measure in order to see how you are meeting or not meeting your strategic objectives. So we'll be adding -- we'll be changing the course from a one- to a two-day course.

We also found that giving the participants more time to share with everybody in the room what they had come up with, instead of just a few here and there, that just is going to enhance the education opportunity for everybody who attends, and certainly will help us enhance our ability to further develop the course and the materials that could be used by the community.

We are hoping to have a public course offering out in the next few months, so definitely stay tuned for when that first offering will be. We will be looking to do courses in both Pittsburgh in the Arlington, Virginia area. But also we'll be doing some other courses geographically located throughout the country.

So as those are scheduled, they'll be put up onto the page. I'm very excited to keep this moving on, and I think that this is an area that is going to be very well received by our community of interest.

Part 4: Customer Experiences

Julia Allen: Great, Michelle, thank you for that preview. And Lisa, before I close by providing sources where our listeners can learn more, I'd really be interested -- I know you and Michelle have been very actively engaged with many of our customers, and working with them to help improve all kinds of aspects of their risk management and cybersecurity programs.

Could you briefly say a little bit about how this works -- this measurement workshop and the GQIM approach -- is showing up in your customer engagements, to the extent that you can talk about that?

Lisa Young: Sure, I'd be happy to. So, one of the things that we get asked often by our customers is to help them build a better risk management program, whether that's an

operational risk management program or an enterprise risk management. And they often couch the discussion in, "I want to be able to quantify my risk."

And so by definition, building a risk program involves measuring things, right, and setting up your metrics? So one of the things that this workshop provides is some of the foundational elements that need to be in place for a successful risk quantification program, which is just another way to say, "I'm measuring something."

It just happens to be, in this case, risk. But this method -- I think the thing that I like about it and what people really gravitate towards, is that it can be used for any type of program -- security planning and management, IT operations, business continuity, disaster recovery. So it has broad applicability across many different disciplines. And I'll stop there and ask Michelle to fill in, because we have been using this method a lot with our customers lately.

Michelle Valdez: I think that one of the advantages is -- everybody's in a resource- constricted environment. And finding out what is the right data that is needed in order to provide senior leadership and executive board of a corporation with the data they need in order to make the right business investment decisions is critical.

So having a framework that people who are at the operational level can use to help them to tie what they're doing and looking at on a daily basis into the terms in which they can then get information and make requests up to their C suite and their board on what kind of investments they need, in the business terms that their C suite and board understand, I think has been just huge.

I mean, it's what has been so well received by the customers that we're engaging on a daily basis, because they've been frustrated in trying to communicate their technical requirements in a way that the board understands.

So by helping them understand that they need to be tying what they're measuring and the things that they're doing to the strategic and business objectives of their organizations I think was an aha moment for them. And it's something that has been very well received and I think is a common problem regardless of the type of industry that people are in.

Julia Allen: Great. Well, thank you both very much. So Katie, I'll give you the last word since you've been so key in developing our facilitator's guide and in telling the story of our workshop. So do you have some places where our listeners can learn more about this content?

Katie Stewart: Yes. So, our team is in the process of publishing a technical note with the very creative title, "Measuring What Matters Workshop Report", which gives an overview of the workshop, goes into detail on a lot of the scenarios we talked about, as well as the GQIM method. That should have all the information on both the workshop, the outcomes, as well as next steps.

Julia Allen: Right, and when that report is available we will include a link to it in the show notes, and Michelle will be making materials available as we formulate our scheduling for our public course.

I also wanted to mention to our readers who have followed this resilience measurement body of work that we do have a number of technical reports on our overall approach to resilience measurement, including this GQIM strategy, and I'll include links to those in the show notes as well.

My dear colleagues, I can't tell you how thrilled I am to have had this opportunity to work with all of you, so let me start with Lisa. Lisa, thank you for your thought leadership and for giving us an opportunity to put a stake in the ground and pull this all together for the ISACA conference. Really appreciate your participation today.

Lisa Young: Let me say thank you to all my colleagues, as well as a big thank you to ISACA. They were instrumental in allowing us to craft this workshop for their constituents. So we were very pleased and they were very supportive of us throughout the whole process.

Julia Allen: Great, and Katie, thank you for your leadership in capturing all of our instructional materials on how we were going to move this work forward, and the workshop report, and all the work on strategic objectives. So thank you for your participation today.

Katie Stewart: Thank you, and thank you to the rest of my team. This was actually a really fun effort.

Julia Allen: And Michelle, our fearless leader going forward, thank you for everything that you did, all the scenarios, and pulling all the workshop logistics and materials together and making this happen, and your willingness to lead this effort going forward, to turn this into a CERT public course. Really enjoyed having you on the call today.

Michelle Valdez: Thank you. I'm very excited about where this is going and the opportunity, and thank you to such a wonderful team. I agree with Katie, it was an amazing effort, and I truly thank ISACA, because without being able to do the workshop for their ISRM conference, we wouldn't be moving forward where we are now and making this available to hopefully lots of people.

Julia Allen: So thank you everyone.