Train for the Unexpected
Transcript

## Part 1: Steering Committee Sponsorship; Risk-Driven Training Topics

**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 operational resilience and software assurance. Today I'm pleased to welcome Matt Meyer. Matt is Vice President and Business Continuity Manager with Marshall and Ilsley Corporation. And today Matt and I will be discussing a process, an effective process that he's been using for training and awareness, and the role that this plays particularly for business continuity and operational resiliency.

As a point of information for our listeners, Matt's organization has been working with CERT for several years to develop and pilot the CERT Resiliency Management Model, and organizational training and awareness is one of the twenty-six process areas in the model and we have captured podcasts on the model and in a couple of other areas which you may want to listen in on. So welcome Matt, really glad to have you with us today.

**Matt Meyer:** Well, thanks for having me Julia.

**Julia Allen:** So I don't think you'd get many arguments that people would say that awareness and training is important for a variety of things, information security, business continuity, operational resiliency, pick your favorite topic. But it tends to be kind of a tough sell at times in the press of day-to-day business demands. So what ways have you found to be able to get your own, and maybe your observations of other organizations', business leaders behind an awareness and training program?

**Matt Meyer:** Well, this might sound a little bit obvious, but for us, the first step that we wanted to take is to make sure that our senior leaders within our organization were behind the business continuity and resiliency program itself. We wanted to make sure that the senior management here understood the scope of our entire program, and in the context of that program then, understood the types of training that we wanted to implement, how it could affect the bottom line. And by bottom line, they're most concerned with how is that going to reduce risk for us. So we had to make sure that we illustrated that to get them to buy in on our program itself. But then ultimately I think really it's just the best way is to make training and awareness a main component of the resiliency program, rather than trying to sell it separately or as an add-on to be approved after the fact. So we really baked it into our program.

For us, there's a couple of different ways I think that you can get senior leadership to buy into the program and get that support itself. And we're very lucky over here. We were blessed with getting a business continuity steering committee together. And that steering committee is made up of a number of senior managers across the organization that represents all the key lines of business, and a number of the support groups. And that group is committed to spending time on business continuity and resiliency. And so for us it was really a natural fit to take a look at training and awareness elements as part of that support, as part of that program. And because

they're so familiar with the program and are on board with it, it was just natural for them to buy into the training piece of it as well.

**Julia Allen:** So what I gather from what you're saying is ultimately you want this woven into your mainstream program, your business continuity program, your operational resiliency Program -- the normal, day-to-day business ebb and flows so it isn't treated like a special project right?

**Matt Meyer:** Exactly. If it's treated like a special project then I think we'd have to come back and get approval year after year, where we know within our organization that business continuity is important, resiliency is important, and they know that as part of that, we've got a training component that has to be done. How we do that training is up to us, with their approval and support of course, but that training and that whole program is supported and that's just a piece of it that comes along with it.

**Julia Allen:** So Matt, you said something kind of intriguing when we were talking about my first question, and that is putting the awareness and training program in a risk context. So I'd like to pursue that a little bit further in my second question for you, which is how do you actually go about building up the needs, the awareness and training needs, and determining which are most important? I suspect there's a risk element to that aspect.

**Matt Meyer:** Yes and it's going to be different, I think, no matter what type of an organization you're in. Obviously being in a financial industry we have certain type of risks that we want to focus on to identify what's most important. But here, what we wanted to do when we started developing that training with the program is we really took a step back, took a look at our entire program across the board and said "Okay, here are the major elements of our program. And here are the opportunities within that program that we have that we can create some training around to increase our resiliency." And when we look at that there's a number of factors that we want to look at, risk being one of the larger ones.

So as we do that we are able to identify those training opportunities that made the most sense to pursue, then develop the training curriculum around it -- what type of training that we wanted to do, whether it's hands-on training, computer- based training, webinars; we do a number of different things over here. And then we can prioritize it and that's where, I think, risk really comes into play. Because we, and just like any other organization, I don't think you really have the time to do all of the different types of training that you want to do. And so we took a look at where are we going to get the biggest bang for our buck or in some cases, just where is our greatest risk, and focus on those activities. Try to get those training elements completed first and then move onto the next one.

**Julia Allen:** Okay, that makes sense. That's a decision process that you would use to apply to any investment requirement where there's demand for more resources than you have. Do I have that right?

**Matt Meyer:** That's exactly right. And it's interesting because one of the things that I talk about a lot when I talk to folks about training -- and you'd be surprised at how often this comes up in professional meetings. Our organization puts a high premium on life and human assets. And so it was surprising when we went to our senior management team and said, "We want to make sure, for all of the facilities that we have across the organization, we want to make sure that everyone's safe. We want to make sure that they're practicing evacuation drills, know where to assemble, know how to get out of the building, etc." and they were very supportive to do that. And it worked well in our training priority as well, when we were trying to get some of these elements through, because it was an easy thing to get out there and get employees involved in

believing that "Hey, this is a good thing, I'm glad you guys are showing us that we need to do this." And it has some immediate payback when some sort of an event occurs.

## Part 2: Involve Key Stakeholders; Follow a Defined Process; Collect Metrics

**Julia Allen:** Excellent. So as you're putting your training, awareness and training needs, programs, objectives together, who are some of the key internal and external stakeholders -- some of the key roles who you make sure are involved with you, either throughout the entire process or at key points in the process, including your sponsors, maybe some of your external partners, your actual students. How do you identify and build that stakeholder body?

**Matt Meyer:** Well, if we talk about internally first, and I said it before -- I think for us it was really critical to have senior management sponsorship. We felt that we weren't going to get a single thing done without that. And it worked out well here. We were able to build it from the ground up with our steering committee. So we had that support that we needed, where they didn't necessarily need to actively participate in all the training. They needed to make sure that they visibly showed support.

And then as far as actual participants, we really do try to make sure that everyone is involved in some shape, form or fashion, depending on their role. Obviously some folks aren't going to have a lot of involvement but there's others that are going to have quite a bit of involvement. And we have, when I step back and think about it, we have a lot of different types of training activities that we have geared towards different levels of the organization. I mentioned evacuation drills, which touches just about everybody. But it's important -- they need to all know how to get out, they all need to know how to assemble, or where to assemble, how to be accounted for. And then we also have floor captains, or some companies call them floor wardens, and their responsibility is to try to help people get out of the building. We need to make sure that they practice that activity.

We also have throughout our footprint, we have regional crisis management teams. Those individuals -- it's senior level people in each region that would really be responsible for managing crisis situations in the region. They need a much of a very hands-on I guess, type of an approach on what they need to do. And so we physically go out to each of the regions, sit down with that team, we start out with a little PowerPoint presentation, make sure they understand the basics of their role, their responsibilities, etc. And then we actually walk through a crisis situation, do a little tabletop exercise to illustrate "Hey, here's why we talked about this stuff in the presentation, how it's going to help you, what tools you have available to you to help get us through that." And we just have so many different types that we use to fit the given situation.

I think, at least for us, one of the most important things to do are those exercises. I mentioned the little tabletop that we do with our crisis management teams. But we perform a lot of workstation recovery exercises and we consider that training. We also perform a lot of technology recovery exercises, building back data centers, etc. -- that's considered training. And those hit a lot of individuals just because of the number and the volume of exercises that we do here.

From an external perspective, it's interesting you ask that, because I think people don't always think about that. It's important but it's not always included in a training and awareness program. And because I think sometimes it's just not that easy to first of all identify "Hey, who needs to participate?" and then be able to get the right people to the table. But we try to do it where it

makes sense. We look at our training activities and say "Okay, is it appropriate to bring somebody to the table for this?"

So for evacuation drills we do involve the fire department and the police department at least for our larger buildings that we go through that with. But we also take a look at trying to actively involve some vendors in our technology recovery exercises. And this is more on the awareness side, but I am a firm believer, and our company is a firm believer, in being involved with public-private partnerships. Now they're starting to pop up all over the place. I'm sure you've got one in your region. But here, at least in southeastern Wisconsin, we have an organization called the Southeast Wisconsin Homeland Security Partnership. And it's a great venue to get to meet the people in the public sector and understand who they are, what role they play in any given crisis situation. And we really are trying to spread the word to the rest of our footprint to get people involved in that.

Again, that's not what would be considered an official training exercise for us. But it is a key awareness piece, that we know who some of these high level emergency response folks are that can help our organization get through this types of events in the region.

**Julia Allen:** Excellent, excellent. Well, I think you've touched on a couple of important key steps in the process that you are using for putting a new program in place and hopefully keeping it current as it rolls out and is taught to various groups. But could you briefly walk us through once you've decided that a training and awareness need is top of the list, and you need to put a program together, how you go about doing that?

**Matt Meyer:** Sure, sure, and I think I did talk about many of these, I'll try to take a step back and put them in order. The first thing, and you may have heard me say this, is getting support for the program, getting that senior --

**Julia Allen:** Yes, so I think emphasizing it is probably a good thing because without that there's no foundation right?

**Matt Meyer:** That's exactly right, so we can't emphasize that enough.

But once you have that, and assuming that you've got that support, then it's just taking the step first of all to identify where that education is required, where that training opportunity exists. There can be so much but you have to really limit it in any organization. So figure out where it's going to be, where is it going to provide value both to the employees and to the organization itself.

And then once those opportunities are identified, I think it's important to understand what specific activity, training activity, is going to be most appropriate for it. In other words, "Gee, should I do some hands-on training or will a CBT (a computer-based training) activity suffice?" etc. Then go through and develop the actual training activity.

Something that I think is lost but I, in many programs is lost but I feel is very important is develop some sort of a tracking mechanism or some metrics for each training activity, understanding, at least at a basic level, what is the activity, when was it completed, who participated, etc.

**Julia Allen:** Well, I would assume -- you mentioned metrics, which is a topic near and dear to my heart -- and that is I would assume that the training need was identified based on a

business need and I would assume that some of the measures that you do need to capture is "are we meeting, have we met the business need," right?

**Matt Meyer:** Oh it certainly is, it certainly is, I think that really does go hand in hand. We hope that we're not going to be training on something that doesn't meet a business need. And that really goes back to that identification stage, make sure that it's in sync with the business. Unfortunately senior management, fortunately or unfortunately I guess, senior management really is focused on ROI. And taking somebody's time to do any form of training is, well, that's a resource, and it's time that they could be doing something else. And we want to make sure that the time that we have them spend on training and awareness provides them a not just benefit to the organization but certainly is going to help us reduce some risk and apply to the appropriate area of the business.

**Julia Allen:** So were there any of the process steps that we missed before I move on?

**Matt Meyer:** The only other thing is the maintenance cycle of it. Once you've gone through and done all that, I think it's important that each one of those things get revisited. So you do want to, as you're going through the years, through your training program that you make sure that they continue to be appropriate, that meet business needs. And as you experience actual events that you understand where things can be modified and improved upon.

**Julia Allen:** Ah yes, the actual events, the teachable moments, right?

**Matt Meyer:** Yes, very important, things that we don't want to happen but are very valuable when they do.

## Part 3: Assess Based on Actual Events; Train for the Unexpected

**Julia Allen:** Right. So, you mentioned metrics a bit, but do you have any formal process for assessing the effectiveness of particular offerings? I mean I suspect you ask your students to fill out a survey and collect the standard feedback, but how do you keep your offerings fresh, on point, relevant to the needs of your students?

**Matt Meyer:** Well, there's a number of ways that we can do that. And it can be kind of challenging because a good training and awareness program is fairly comprehensive and it's fairly large based on what the business needs are. But for us, one of the key things is making sure that within our metrics and measurement we have created a good foundation, that good baseline. So that as we move through that and conduct our training we can benchmark against it, based on either feedback from the groups themselves or, we touched on this a little bit, the actual events that occur. Because when an event occurs that's really the best way that you can determine whether or not that training component was effective. They're going to help you identify gaps in your program and identify the improvement areas.

I talked a little bit about evacuation a couple of times and to me that's one of the easiest ways to show how improvement can occur, and one of the easiest ways to show how the process can happen. Here at M&I, if we have an actual evacuation for whatever reason, it seems like we've got employees that like to burn popcorn and of course the fire alarm goes off, everybody evacuates. Years ago, everybody would just come back in, you'd forget about it, it's over with. Now we have baked into our process that when that occurs we get together with that group of floor captains or floor Wardens -- they're the ones that are responsible for helping make sure that the building was evacuated and that people are accounted for afterwards.

We get together with them and talk through what just happened -- what went well, because we do want to know that, but also what were the problem areas. When people got outside did they decide to go to Starbucks instead of going to their assembly location. And it really gives us an opportunity to say "Okay, where in our training program, in our evacuation drill process, did we miss the boat? How can we fix this?"

And it seems like such a simple example but we can take that process and apply it to all sorts of things that occur within our organization. And it really can be considered part of problem management in a lot of ways. But just the art of, and the ability to take a step back soon after things happen, get the right people together, and walk through it, and say "Okay, where did we go right, where did we go wrong in our training to prepare people for this?"

**Julia Allen:** Right, but I think the pivotal thing that you said that enables that to happen is you also have that baked into your process. In other words, you don't have to remember to do it, it doesn't have to be somebody's good idea to do it, it's not an ad-hoc action, it's "Okay, we're in the midst of this process, here's the next step, and we need to assemble the right people and get to it," right?

**Matt Meyer:** Exactly, and that's difficult to get to that, because it's time consuming. And generally when it's going to do the most good is right after the incident, and people aren't always -- they don't feel like they have the time to do it. So it's challenging, it's challenging to bake that into your process. And I encourage folks to not give up if they try to do that within their organization, and it struggles for a while, and you take a couple of steps back before you can take a step forward. I know it happened here, it's probably going to continue to happen, but all in all, it's an effective process and it continues to work.

**Julia Allen:** Great. Well, as we come to our close Matt, we're talking about operational resiliency, we're talking about business continuity, really with many multi-dimensional, with many issues and risks to tackle and resolve. So what do you believe is the role or the relationship of training and awareness when it comes to you and your colleagues being able to say, "We're achieving our business continuity, operational resiliency objectives at M&I," how does training and awareness help you get there?

**Matt Meyer:** Well, it really goes hand in hand. There's the old saying "Practice makes perfect," and this is certainly a good example of that. When we started talking about recording this podcast and that potential question was discussed, something came to mind.

I've got a brother who works for a large fire department, and I think firefighters and fire departments are a great example of illustrating the importance of training and awareness and how it relates to resiliency. Because if we think about it, firefighters are called upon to go to unknown situations and are expected to deal with them effectively. It's not just fires that they go to and they go to a multitude of different things and every situation, even if it is just a fire, it's different no matter where they go.

And they take the approach that they need to continue training their staff, their firefighters, to be able to handle any given opportunity. They don't expect to have to train them on every single thing that occurs, but they want them to be resilient themselves, to be prepared to deal with whatever they would come across. And that's what they focus their training on and they do a fantastic job of that.And if we in the private industry can do that with our employees to be able to make them that operationally resilient -- that they can walk into a given situation, be able to quickly assess and identify what some of the issues are, and work through them, and understand how their actions are going to help, I think that's just invaluable.

So I really see that relationship of training and awareness and resiliency as being one of the most critical ones that we have as an organization.

**Julia Allen:** Well, I really like your example with firefighters and also being resilient individuals trying to bring resiliency into an organization. Because, as you say, we often don't know what the situations are and the question is are we equipped to deal with it whatever it is and ask the right questions and get the right people involved in the time that we have to, right?

**Matt Meyer:** That's exactly right.

**Julia Allen:** So Matt, do you have some resources that you particularly like or would recommend where our listeners can learn more on the subject?

**Matt Meyer:** Well, I wish I could tell your listeners, “here's a specific website to go to, or a book or a pamphlet,” but what has worked for me -- and I really would encourage other people to do -- is to network.

I really think that the best way to find some good fresh ideas is to network with some people that are in your profession, get involved in local professional organizations. We have a number of them here in southeastern Wisconsin that I attend. Get involved in a local public or private partnership. Or just talk to some fellow professionals to find out what they've been doing, find out what's worked for them, what hasn't worked for them, why they worked, why they didn't work. And then you can take those things that they talked about and figure out "Okay, what's going to work within my organization." And it's not just a matter of "Hey, I got this idea from Bob and it worked for him, it's definitely going to work for me." That's not necessarily true. Every organization is a little different and you might find a great idea that somebody said "Well, this just didn't work in my company because the culture didn't support it." But you may realize "Wow, that probably is going to work really well for us." So just talking and working with those folks I think is one of the best things that can be done. And there's a ton of resources in most cities where you can get involved and talk to people just to find out what's been done and what's worked and what hasn't.

**Julia Allen:** Well, and it sounds like you also recommend taking as many lessons as you can from related disciplines like firefighting, emergency response, any type of organization that gets involved when there's a local, city, statewide, even federal event -- taking a look at some of their procedures, processes, and training. Would you recommend that?

**Matt Meyer:** Yes, it's amazing what you can learn. And that's -- I found our local public-private partnership invaluable as far as that's concerned, because there are so many different disciplines at the table that we can work with. We've got, from the public sector, we have public health, fire department, police department, emergency management. It's just incredible the types of things that they do that we in the private sector don't always think about, and that we can take bits and pieces of that to improve our own program. So I certainly recommend that to anybody.

**Julia Allen:** Well Matt, I so appreciate your time, your expertise, your thoughtful comments and responses today, and I really enjoyed our conversation.

**Matt Meyer:** Well, thanks for having me Julia.