Bobbie Stempfley: Hello, and welcome to today's SEI webcast, "Organizational Resilience in a Time of Crisis". My name is Bobbie Stempfley. I'm the director of the CERT division here at the SEI and I'd like to thank you for attending. Today I'm joined by Matt Butkovic, one of the tech directors here. Matt, would you introduce yourself and talk about your role here at SEI?

Matt Butkovic: Good morning, Bobbie. Absolutely. So, as Bobbie said, my name is Matt Butkovic. I lead the Cyber Risk and Resilience bodies of work here in the CERT division, and today, Bobbie, looking forward to a discussion of a topic that's near and dear to my heart, which is organizational and operational resilience.

Bobbie Stempfley: I think near and dear to both of our hearts, so really looking forward to this conversation. We want to make (inaudible) the conversation here, but I want to include you, so feel free to put your questions in chat and we will work hard to get to all of them over the course of the next hour. This topic of organizational and operational resilience is important in any day, but I think it's even more important in this moment of uncertainty that we're currently experiencing. These crisis efforts where you thought you'd planned for things and maybe your plans either work or don't really bring to the forefront the fragility in a variety of things. So it really seems timely to focus on this and I think, Matt, I want to get us started by talking about the term "organizational and operational resilience". These are really big terms, and you've really thought deeply about this. Where do people start wrapping their head around how to approach something like operational and organizational resilience?

Matt Butkovic: Certainly, Bobbie. So it is a big term, or a big concept, but I think we can start small with something that’s relatable. Let's first examine what we mean by resilience. Resiliency is the ability of an organization or a person or a system to come back from a deformative event. So let me use an example or a metaphor or an analogy, depending on the way we couch this. So I'm assuming, Bobbie, that as a child you likely had a Slinky, as did I.

Bobbie Stempfley: Several of them.

Matt Butkovic: Several, right? And you and I are of the age where our Slinkys were metal, not plastic, and that'll become important in a second here. So we had Slinkys, and if you did what I did, you took one end of the Slinky and my brother took the other end of the Slinky and we ran in opposite directions, and suddenly we didn't have a Slinky anymore, we had a bent piece of wire. It would slink no more, right? So it was never going to walk down stairs or go around corners like the commercial.

Consider resilience, operational resilience and organizational resilience, in the same light, which is you want your organization, or even a specific person in your personal life-- you want to be able to flex and pivot and come back into shape just like that Slinky. What you don't want to do

is exceed that operating limit, and once you've exceeded the operating limit, there's no coming back. That's when the organization can't go back into its intended form.

A few things to consider. All organizations have an outward bound, and thankfully most of us never find that outward bound in our personal life, and most organizations don't find that outward bound in the course of their business. I would argue the combination of stressors and disruptive events we're facing right now is putting people and organizations on that edge. So a long-winded way of saying operational and organizational resilience is a set of concepts intended, designed, and delivered to ensure that you can meet your mission. That mission can be creating something-- let's say you're a manufacturing organization, or the purification of water, or it could be delivering educational services if you're a university. Every organization has a mission and that mission is underpinned by key things it delivers; and then those things, those key services, are enabled or underpinned by assets, and we can talk about that in a minute, but let me go back to you, Bobbie, and see if my explanation is holding water so far.

Bobbie Stempfley: Yeah, I think so. I think the one question that is really important in today's world is how do you think about resilience and change at the same time? So maybe later we'll explore where those two concepts come together and where they maybe create a little bit of (inaudible), because I think that when we're pushed to these limits, to the outer bound limits, it's important for leaders to help organizations to not just survive but also take advantage of how to pivot in that moment as well, and that can both be a benefit to resilience in an organization, but I think any change creates and magnifies stress, and so I can see organizational resilience being an important element there as well.

Matt Butkovic: Sure, Bobbie. So let me, before the thought slips away-- resilience and change are interwoven, right? So to be resilient, you must be able to contend with change, and ideally anticipate change, so that you're not in a reactive mode. So if we think about organizations or we think about our own lives-- and I think that unfortunately the COVID crisis has made us think about our personal exposure to risk in a way that many of us would typically avoid or kind of table that thinking. But if you think about decisions we're making now about interacting with groups of people or visiting certain locations that might be of higher risk, we are managing our exposure to a specific type of threat, and that threat is the virus. The same goes for organizations in cybersecurity and the physical world.

So when we think about operational, organizational resilience, we have an obligation to manage the conditions we expose ourselves to-- so deciding not to go to a crowded theater-- and then managing the consequences. If I go to that crowded theater and I may be ill, how do I deal with that outcome? So the same applies for organizations, managing conditions and managing consequences. We all know you can't comprehensively protect yourself from all threats, therefore you can't mitigate all risk, but you have to make risk-informed decisions that allow that portion of risk that you experience to stay within your risk attitude, tolerance, and threshold.

Bobbie Stempfley: So (inaudible) risk tolerance and threshold concept a little bit, because I think the first thing we should do is tease apart the differences between risk threshold and sort of a tolerance activity, because I think that's a really important distinction. How does an organization think about risk and its areas of risk and its tolerance for assuming (inaudible)?

Matt Butkovic: Yeah, thanks, Bobbie. I think it's really important to parse it the way you've described. So an organization has a finite appetite to do things that might endanger the organization, and the same for individuals, as we were exploring. So you have that specific limit, and that's the threshold, and if you exceed that threshold, you're now engaged in activities that represent a risk greater than your appetite. So these are things that should be avoided; or, if they can't be avoided, they should be well understood and the effects mitigated. And then there's a population of things that fall below that threshold, that are within your appetite range, that are within your tolerance, is probably the best way to describe that.

So you have to consider each of these on their own and in combination, and I think this is an important element of today's discussion, which is entitled "Operational Resilience" or "Organizational Resilience in a Time of Uncertainty", in a time of COVID. In essence, I am increasingly worried about those combinations of threats, and I know, Bobbie, you've got some thoughts on this as well.

We're in a situation where your workforce is disrupted physically because of the pandemic, but thankfully we haven't seen the waves of cyber-disruption that we may have anticipated, but that doesn't mean they won't happen. So I have a question for you as a follow-on there, but I just want to put this idea on the table, which is organizations can't think about these risk categories in isolation. That doesn't make a lot of sense, right? To do risk management well, to ensure you're not exceeding that threshold, to make sure you're staying within the risk tolerance parameters, you have to think about the interplay of physical and digital, and from a resilience perspective, that means thinking about four basic asset types: people, facilities, information, and technology. And if we think about that list, that current crisis or set of crises we're dealing with are disrupting multiple assets at the same time, but the cyber or the information and the technology asset, those have been largely unimpaired by the current events of the day.

My worry is that you could then see an amplification of crisis by a large-scale cyber event disrupting those assets in addition to the others, rendering even more difficult the task of meeting your mission. So Bobbie, I know you've had a variety of roles where you had to think about assets and think about mission. I think it's safe to say that as cybersecurity practitioners we have become really used to giving sort of a pat answer on how you look at cyber risk, right? We've gotten good at analyzing the relative likelihood and impact of those cyber risks. I would argue-- and I wanted your thoughts on this-- I think that cybersecurity practitioners struggle at times to join what we know in our discipline with the folks that focus on physical risk and physical

security, and this pandemic, and the loss or the impairment of facilities, has had us thinking about those things in a way that probably wasn't front-of-mind a year ago for most folks working in cyber.

Bobbie Stempfley: Yeah, I think you're right, although I think there are places where we need to be more precise, and that is if you look at the global digital enterprise, you're right, it has been shockingly resilient, to use that word, in this pivot that everybody has happened. But I don't think everyone has experienced equally the cyber risks that have occurred here, and so I do think there is an uptick in some malicious activity that's going on and I think we should be really careful not to broad-brush in that activity, because any kind of crisis creates even more stress on those least prepared to handle the crisis, which tend to be those that have prepared the least or who have the limited amount of resources to adapt in this situation, and I think this one as well, against those four asset classes, has done the same thing. Everybody has assumed a particular operating model, whether it be in a facility or leveraging a facility. They've built their supply chains to operate in a particular manner and we've not perturbated those and it's taken a little while for them to come back.

I like the generality of those four assets classes-- humans and facilities, technology and information-- because that lets you draw back to the common language across cybersecurity, physical security, business continuity and others, and that is the business or the mission of the organization, and you can really-- if you start there, then you do have that common language across all of the different individuals, and as cybersecurity practitioners, we have had a history of getting very detailed very quickly about what's going on in the tech and we need to make sure that we can have an effective communication about how that impacts the business or the mission, and I think that's why so much of this idea of organizational resilience and operational resilience has to start at that level, right? How much risk will you accept to the business or to the mission? And in some areas it's none or a very small amount, and others it can be a large amount, and so that idea of differentiation I think becomes really important and speaks to the need to have preparation and practices in place. How do you-- please, Matt.

Matt Butkovic: No, I'm sorry, Bobbie, I'm just eager to build on your point and reinforce it. So it may seem reductive to talk about only four asset types and key services, but there's a power in that that they've described, which is if you can boil it down it makes it easier not only to kind of understand the interplay between your critical services, your mission and your assets, but it allows you to take substantive action in a way that's much more productive.

So if I said, "We're going to change a bunch of stuff in a generalized way that affects technology assets," it's kind of hard to measure how much you've done and what the impact is. I would argue that to make fundamental changes in the way we protect and sustain assets, be it the data center or particularly parts of the technology set, or people, we need to action those things at an asset level. So just kind of reinforcing the point that for those maybe unfamiliar with the way

that we look at operational and organizational resilience at the SEI, there is a specific logic as to why we assign and group assets in those four categories, and why the list may not be as expansive as you might assume, because we do see a power in being able to boil it down and reduce to the fundamentals, right? And I think that something that the current crisis is teaching us is that mastering the fundamentals really matters.

So one of the ways in which I think the COVID crisis and cyber are similar is that both affect multiple geographical locations simultaneously without regard for border. Right? So if you think about natural disaster, going back to that description of maybe physical security not being front-of-mind for cybersecurity practitioners, it's unlikely for organizations that have any geographic disparity that a single event is going to simultaneously affect all of their locations, globally. That happens in cyber and is happening with COVID, and I think it's interesting to see the way that the two communities now have kind of a mutual understanding of why it matters, why you have to prepare for that scenario.

So just wanted to not engage in a ramble but I wanted just to kind of reinforce the point that understanding your operational and organizational resilience at the asset level is very important, and I would argue that the current crisis is teaching us lessons, or reinforcing lessons, about how comparable a threat can be both in the physical world and in the cyber world.

Bobbie Stempfley: So I think two things are important. One is those four asset classes are the top level, right? You devolve within those down to more detail. So it isn't about simplifying it to the point of making the problem seem less important or less complex than it is, but it is about giving you a common language. I also think it's important-- we have a question about thinking about the new normal. When we think about how we build and sustain our resilience programs in organizations, how then you bring in the lessons and you say, "Okay, I want my new normal to be more of a remote workforce," perhaps, or more of a change of my technical architecture. So I put this new technical architecture in place to support the operating model that's today. That's now my new normal. How do I bring that back into my organizational business continuity and resilient functions?

So you've done several-- helped people go through the establishment of their programs. You've done some of these yourself. Perhaps you can give us some lessons from your experience.

Matt Butkovic: Yeah, thanks Bobbie. So I'll draw on my experience both at the SEI and then when I was in private industry. But a thought, first, if I may, about the new normal. So I think maybe we should scrap the idea of a new normal. Certainly we have a new way of working or a modified way of working, but I think that looking at these as normal and abnormal or standard and non-standard is probably counterproductive in the long run for us-- and I know that's not your term, Bobbie, it's a term that we're all using these days-- but I was thinking about this last night.

So I think it's more productive to think about modes of operation. So the immediate new normal is your workforce is highly decentralized, working from home, drawing on, depending on infrastructure not owned by the organization primarily, which is fraught with new risk. Do I think this will be the way of working forever? No. I think we're going to come back to some middle ground where we have a larger, more robust remote workforce, a work-from-home force, in most organizations, but certainly we're still going to have offices and we're still going to have data centers, and all those things are still going to be there. So I think we're in this sort of early honeymoon phase of the new normal.

With all that said, organizations need to think about that mixed mode. It's not just standard operations and disaster recovery, it's now this perpetual blended hybrid mode where a certain percentage of your workforce will need to toggle on the ability to work from anywhere in a comparably secured manner, perpetually. So the really good news is-- I mean, think about what we're doing today, right? You're in Virginia, I'm in Pennsylvania, and we're having this webcast globally, and we did this with relative elegance, using the equipment I took home when I left the office on March 12 of this year. So the technology has caught up in a way that allows us to do business continuity and process continuity in a way that was very difficult before we had ubiquitous broadband and before we had virtualization of systems, and applications like Zoom and Skype.

You asked about lessons learned. One of the chief lessons that I learned doing business impact assessments in private industry and working for organizations with the SEI is that there's a temptation to focus on the movie plot stuff, and what I mean by that, I think of a very specific example when I was in manufacturing. I remember executives being very excited to buy satellite phones and solar blankets and talking about EMP attacks, and my question was: Well, what happens if this factory in the Midwest burns down?

So I think, to kind of build on the theme, Bobbie, start in a way that's digestible, and focus on a set of things that you can get your head around, and that's where the four asset types come back. It's not that we're stopping at saying information, technology, people and facilities, but rather those are categories, and those categories are the matrix. So let's say-- in my past life I worked for a manufacturing organization, and at the time in North America we had something like 1100 products. That database server and that production control equipment wasn't used exclusively for one of those, but rather across that stack. So I think, again, anticipating some disruption in your operation requires you to think then about the assets that comprise that operation.

Another pitfall that I've seen is a focus not only on sort of the movie plot stuff-- the comet hits the factory or zombie apocalypse-- but rather a lack of focus on return to work, and that was I think the second part of the question you were asking. So once you go into a non-standard mode of operation-- and I think we should probably draw a distinction between the work-from-home

situation we're in now and a true loss of data center or loss of production facility, which then invokes alternate resources in a much more substantial way. But once you're using those alternate resources, once you've gone from the primary data center to the alternate data center, for lots of reasons, both operational and financial, you need a plan to go back. You can't stay in that mode forever. And I saw lots of organizations, and my (inaudible) the time-- and we corrected this-- was focused on going to the DR site, invoking the business continuity plan, with very little thinking about resumption of standard operations.

So I think COVID is a variation on the theme. As I mentioned, essentially we're dealing with a distributed workforce in a way that's new and novel, a scale that's new and novel, but they're still doing the same things, basically, with technology that we had in hand, which is different than, "Oh my, the data center caught fire and now we need to cut over to the alternate site where our throughput is different, it's potentially a different staff, remote administration looks different, we're not journaling certain transactions in our production systems. All of those nuances needs to be thought through because without that, it's difficult to ever return to normal operations.

I'll just share a quick story about that. Did a business impact assessment for an organization in the U.K., and they'd recently moved from one enterprise resource planning system to another, and the new enterprise resource planning system was state of the art, state of the art to the point where no one knew how to then restore transactions that were performed while the system was offline. So basically the answer was: If something bad happens to SAP, stop the factory because we can never get the information back into SAP.

It's those sorts of gotchas with information technology that organizations need to think through. I describe it as the "We've got good people" fallacy. It doesn't mean you don't have good people, right? You have lots of good people. But the idea is something bad happens, a system breaks-- "We don't need a DR plan. Disaster recovery will take care of itself because we've got good people." It doesn't matter how earnest and skilled your people are; if they don't have the tools to perform their job, you're going to be in a difficult situation.

So the idea that SAP goes down but the Dunkirk spirit takes over and we're all going to pull together-- that works on a human sort of emotional level, but the technical reality is that you don't have the form stock, you don't have the basic raw materials needed to capture transactions or perform those tasks. So my advice is stay realistic and absolutely engage in tabletop exercises. Make them realistic. Have them span from things as simple as we've had a fire in a key facility through we have a global pandemic. I think that understanding that spectrum of disruptive events is really important because the impact and the way you resume your normal operations are quite different.

Bobbie Stempfley: So I go back to the four asset classes and the first one we talked about was people. Your people have to be resilient in their own right, which means you have to have

systems and infrastructure to enable them and support them throughout the effort, and then you have to also facilities and technology and information to support your business operations as a part of it, and I think that's a really powerful way, and I like the fact that we start with that piece, that sort of people element of it, because I think that's important.

The other one that I find interesting and I want to explore for a few minutes is we've talked a lot about needing to do planning, everything from you have to have meaningful architectures in place. Had this pandemic hit ten years ago, before we had these tools, I think we'd have a very different experience and sort of a different model. Because of all of the advances in technology, in virtualization and in wide-scale broadband capability, we have a greater capacity today. It's not equal-- there are different parts of the country, different parts of the world that have this and don't have it, and I think that's an important thing for us to address from a resilience concept as well.

But I also think-- let's talk a little bit about how an organization that started out making a risk decision, taking on perhaps more technical risk, more infrastructure and information risk, in order to sustain products throughout this time period and is not backstopping that with advanced technology, with supporting their people, and perhaps more or fewer people depending on their business-- how do they go back and shore up that additional risk that they took because this is going to last a much longer period of time?

Matt Butkovic: It's a really good question and I think a probably underexplored topic, Bobbie, which is-- what you're describing in part is now questioning the viability of the lifeboat, or the structure of the parachute. So we've survived the immediate crisis; we're now in this mode-- the longer this goes on, is there an increased risk that the lifeboat starts taking on water? Is there an increased chance that the very safeguards that have seen us through are going to erode over time? There's a familiar concept for cybersecurity practitioners, which is that we're going to failsafe, we're going to ensure that our system is failsafe, but when you're working in this alternate mode, things often also fail open.

So you are taking on additional risk, potentially, and I think you're right-- the advancements in technology have this made this easier. But the truth is there are procedures and controls that you would execute in normal operation that you're probably foregoing in this way of working. I think about additional levels of log review as a simple example, or ensuring that you have periodic maintenance activities executed. So for instance, a number of organizations will delay patching of systems and platforms when they're in this mode. Well, that's fine in the short-term, but eventually you're going to need to do that, because the tradeoff is you've become less secure because you potentially have this unpatched vulnerability. But again, these are all risk decisions.

So, I think your point is a really good one, which is it's not only ensuring the viability of your alternate way of working, but then understanding the limits of that way of working-- when do

you become less secure, in a way that makes systems untrustworthy? So I think that lots of organizations are sort of making it up as they go along because they have to; we're all sort of in that mode. Even the best pandemic planning efforts that I've seen did not foresee a pandemic of this duration.

I'll share with you that I was part of a pandemic planning committee in private industry for SARS and the Avian flu, and the time horizon for that was much shorter. Now, there was a greater expected loss of life, so in some ways it was more dire, but we thought the duration would be shorter. What we're seeing is a tragic loss of life in an extended, slower build, in a way that I think lots of plans didn't account for. So with that said, not to sort of touch on something a bit morose, but organizations have to assume that some of their staff will be incapacitated-- hopefully don't lose their lives in the pandemic, but certainly you have to plan for the loss of key personnel.

One of the things that I saw in the pandemic planning exercises I was a part of is that there's a lot of optimism. The truth is if someone's family is in dire need of medical attention and someone's loved ones are ill, I think it's overly optimistic to assume that the network administrator is going to be willing and in the right frame of mind to perform their job in the way they did before that pandemic. So you've got to look for alternate resources and temper expectations on what folks are willing to endure in support of their employer.

Bobbie Stempfley: So let's take this idea of business continuity and this kind of planning on a continuum, that it isn't, "Okay, today we're here and we're going to plan for a crisis, and then we're going to plan to make a full step back into normal operation," that we're on this sort of long-term continuum effort. What do you think might be the best practices for continued evaluation of your organizational resilience practices? I mean, I see ICS as a cybersecurity community, and different organizations really focusing on communicating with their people, keeping in touch with them, understanding what their supply chains are, and really, in some instances, now understanding what their supply chains are and who the suppliers to suppliers are. But at what point in your planning do you go back and put in place the processes you'd historically had to think about risks and to evaluate them and to incorporate them in your current and future decision-making?

Matt Butkovic: That's a great question, Bobbie. I think we need to look at that as an iterative cycle. So I would argue that organizations have several months of COVID contingency to consider. So it needs to be an iterative process. Your disaster recovery and business continuity plans, or continuity of operations plans, those need to be sort of perpetually reconsidered. The worst thing you can do-- well, the worst thing you can do is not consider this at all, right? Thinking that being lucky is better than being good, right? That's a problem.

The second-worst thing that you can do is fighting the last war, and I see a lot of that with

business continuity planning and disaster recovery planning. So we're dealing with the COVID crisis. We all hope this is a once-in-a-century type event, but the truth is we could see a variation on a theme. Something else could happen that looks very much like this, but not exactly like it. So I think that the best advice we can offer is for organizations to make that list of potential scenarios that are worth considering in their context, fact-checking those and making sure they're realistic-- again, not the movie plot stuff, not the, "Robots are coming to attack the headquarters"-- but rather: What happens if there's a loss of electrical power, or there is a new flu that creates a massive workforce outage? Something that is less significant than COVID but more significant than (inaudible). Create that list; make sure that list is considered in the context of all of the types of risk that you face.

One of the things that I'll point to within Carnegie Mellon where we address this is the chief risk officer program, CRO program, certificate executive program, where one of the things that I always need to remind myself when I'm presenting on cyber risk is that cyber risk is only one of a universe of risk that organizations have to consider. There could also be a temptation in the future to, based on our experience with COVID-- and COVID will pass, right? We will resolve this-- to focus myopically on physical threats related to health in a way that then will blur your vision when it comes to cyber risk. I mean, there's nothing to say that during the COVID outbreak-- to your point, Bobbie-- we don't see a spike in cyberattacks that are disruptive in ways we hadn't anticipated.

So I think it's inventorying and cataloguing the list of risks that matter to your organization, enumerating the threat actors that are most likely, and then doing the basic math that allows you to prioritize. At the end of the day, this comes down to prioritizing a finite set of risks and a finite set of resources to contend with those risks.

So I have a question for you, Bobbie. If my answer was sufficient and I can ask you a question, I'd like to now.

Bobbie Stempfley: Go for it.

Matt Butkovic: So I'm thinking about your role and your roles in the past and sort of the view from senior leadership. Let's assume that we are making widgets and you are the CEO of the organization and I am the director of information security. What question would you want me to answer regarding operational resilience in the time of the COVID pandemic? What's sort of front-of-mind for you? When you look at the essential instruments in front of you, how do you find comfort? If there is one question or a set of questions, what is the most fundamental something I can answer for you to give you confidence in our ability to sustain our mission?

Bobbie Stempfley: It's a really great question, and I think the first thing that becomes really important in that one is to say, "As the security manager, what do you see being the most

different in operating in this model?" Let's presume we understood what we needed in order to deliver those widgets on whatever the timescale is. I would want to know what you thought was profoundly different and why, and I think that's sort of an important grounding conversation to start with, and then we can start decomposing that Why, because I think that's really important, because there are lots of things to be perhaps worried about there.

Matt Butkovic: I think that makes a lot of sense to me, which is you want to understand sort of the net difference and drill into the things we can do to effect that. As we know, there's a long tail to these things, so I think that the lessons of the current pandemic will play out-- and again, I'll caution us to take those lessons in relation to things we already know. So I can already see the headline in the IT and cybersecurity publications that says, "Spending on Cybersecurity Down; Spending on Physical Protection Up", and some sort of panic ensuing, and I think that's the wrong way to look at it. We'll find (inaudible), right?

Bobbie Stempfley: I think you're right, but I think the real question that we've got to come to grips with is how we meaningfully quantify the spending that needs to happen on the total set of risks, and then how, as cyber, we can take advantage of some of the spending that occurs in other areas. Because this idea that physical risk is dramatically separate from cyber risk is really interesting, but in practice, your physical security measures generally are implemented via some sort of technology, and so you're equally complicating your cyber risk environment. So we've got to find ways to capitalize on each other's programs in order to be successful in these situations.

Matt Butkovic: Yeah, that convergence is really important, and I think there's this sort of well-traveled narrative that says, "Well, it's different for cyber because likelihood is harder for us to calculate." Right? Well, yes and no. So when you talk to folks that insure risk, they'll point to an entire canon of literature and techniques for determining the intrinsic risk of things that have limited data. So I think one of the things we can learn as cybersecurity practitioners in this is that these sort of events, the COVID crisis, which may seem like sort of a black swan event, these things really do occur, and they're going to cut across our asset types and cut across our risk management techniques. So the idea that I'm really trying to convey here is that the idea that cyber is distinct and different and unmanageable because we don't have the data is kind of the wrong way to look at it. What we need to do is aspire to gather the data that we need, to your point, to then make rigorous calculations on what works and doesn't work-- what's the return on investment for physical protection in the same vein as what is the return on investment for cyber protection-- and we're not there yet as an industry, and that's what keeps it exciting for us, right? Because we do have these opportunities to develop new techniques and management and measurement methods that allow us to better answer those questions.

Bobbie Stempfley: Yeah, I think the challenge we have is one of speed and of understanding, and that is it's-- I remember a national-level exercise that I had the opportunity to be a part of,

and trying to respond to outcomes associated with this sort of national-level cyber exercise, where there were physical consequences of a cyber event. We see that today, but when we ran that exercise more than-- it was probably close to ten years ago-- it was sort of new to everybody's psyche in that space. So to explain that to respond to-- to reduce the physical consequences in Geographic Location One, we actually had to take action in a geographic location that as a thousand miles away. That was a really difficult concept for folks to grasp. Now today we don't have that-- people can grasp that philosophically, but what we're missing in some instances today is an appreciation for risk managers more broadly about what the particular possibilities of cyber might be so that they can add that to their planning exercise. So really having that-- folks understand things like fires and physical disasters or maybe labor disputes or something of that sort because they've happened, and we need to continue to put in place these cyber scenarios, tabletop exercises and other things, so they can understand the cyber consequences that might occur and, more importantly, so that they can understand the complexity that'll come from these things happening at the same time or at similar times, because I think that's the other piece that we've really got to get more mature about.

The second problem we have is speed, and that is that our ability to collect the data, to make these kinds of decisions in a repeatable way, is predicated on our having not just the opportunity to collect it, but enough data to really represent an appropriate measurement and implementation, and as threat actors change and as risks evolve so quickly, sometimes that impedes our ability to get that kind of insight. And then to create the analogy or the framing so that you can have a management conversation, a leadership conversation, about the people, the facilities, the technology, and the information necessary to execute your business.

Matt Butkovic: I think that's a great point, that we're striving for measures that are predictive, right?

Bobbie Stempfley: Right.

Matt Butkovic: So there's a good bit of arguing over how many angels fit on the head of a pin sort of stuff in cybersecurity, and I think that's largely counterproductive. So to kind of join the concepts you were explaining there, for the audience, focusing on consequence-- so kind of consequence-side calculation-- and then not worrying about the fine-grain details of the threat actor but rather the impact of the realized risk I think is the path we need to pursue, because that'll give us impact of measures that are really important in a way that I would argue are somewhat lacking now.

So yeah, likelihood is going to be thorny for us forever, right? I mean, it's just the nature of cyber, but it should be an excuse. Cybersecurity practitioners-- we need to think beyond that, and then augment or compensate for any uncertainty around likelihood with then drawing up on, "Well, what's the consequence?" One of the things that I'd like to see more of is a focus on

things like assurance cases and safety cases in cyber, not just for physical cyber systems but sort of use broadly. So I think this is a technique from the safety engineering community that many cybersecurity practitioners have never even heard of, right? It's something that's just not part of the kind of generally understood body of knowledge.

That's an extreme example of consequence-side calculations, which is: We have this power plant. The power plant has nuclear materials. If it melts down, it's going to do X. We can't have X happen, so then how do we build these dependent nodes and say, "Here are the things that can't happen to ensure that that doesn't happen." I think applying a little more of that logic to our discipline would be helpful.

Bobbie Stempfley: Let's explore that for a minute. If I think about the ways that business continuity planning can go wrong, how you think you might have a continuity plan and not, or perhaps you haven't started one-- how would you bring this idea of an assurance case into an organization's business continuity planning activity?

Matt Butkovic: Certainly, Bobbie. So I think it comes back again to the fundamentals. This is where concepts like recovery time objective, recovery point objective, maximum tolerable downtime-- these things are universal, so it doesn't matter if the disruption is physical or rooted in some cyber exploit-- these are the measures that matter. So I would say that if you're contemplating a business continuity plan, first of all, understand the business continuity plan is the superset of somethings, and then disaster recovery plans are the subset of somethings that address specific platforms and technologies. That's one of the first distinctions that we all have to agree to.

And that really is (inaudible). It doesn't matter what you do. You could be a university, a manufacturer, or a pizza shop, right? If something happens that disrupts operations, what's the maximum tolerate time you can be in that mode before reaching that outward limit that we started the conversation with, before you exceed your operational and organizational resilience. It really starts there, because at the end of the day that's what matters. Organizations exist for a specific function, and all the things we described, they aren't just kind of loosely affiliated things; they all work in conjunction to meet that end. So understanding your mission and then the tolerable disruption that you can endure is really important.

And it doesn't have to be complicated or expensive. You can do this on a dry erase board, in Excel. I suppose you could do it on the back of a piece of paper if you needed to. That's one of the things I want to make sure we reinforce in all of this, which is if you want to think-- and you should-- about operational and organizational resilience, it doesn't take developing an elaborate strategy. It's as simple as understanding what you do, the things used to do it, and then thinking about the scenarios that could disrupt those operations. So start small. Do this in manageable bites, and learn from the process to make it better so each time you do it there's a lower overhead

associated with it, and there's lots of free tools out there. Many of those-- I'm sure that we'll have links at the end of this presentation to the work here at CERT and the SEI broadly, but certainly there are a tremendous catalog of free resources if you want to think about contingency planning and disaster recovery planning in the larger context of operational resilience.

Bobbie Stempfley: Let's talk a little bit about that idea of operational resilience. It strikes me that a small business or even a microbusiness, this might seem unreachable. It might seem too difficult to start. But when you break it down to what business are you in, that can be a clear starting point that's a part of it. Beyond that, what's sort of step two? What are the processes that you need to put in place to go through that questioning? "What business am I in? What do I need to do to accomplish the business? How long can I function without a failure of some sort? Who are providing those pieces?" Do you need a lot of people? Is this something that you can do-- just the lead individuals? How would you approach that?

Matt Butkovic: Sure. I mean, there are many techniques, and of course we have several that we've authored at the SEI and perform in collaboration with our partners in the federal government, but I would say start really simply. What is it that produces revenue for the organization? What is it that you deliver to the community? What is it that at the end of the day you would describe your organization as fundamentally doing? Start there.

So for a microbusiness-- say we're a microbusiness that sews objects and sells them on Etsy, as an example. What do you? "Well, we create these products and we sell them on Etsy." So what's required to do that? Well, we have the raw materials, we have the ability to then create these objects using sewing, so there's some people involved, and then there's the ecommerce part, where we take this and then monetize our creations on Etsy, we sell them to the public. Well, that requires us then to manage a small inventory, so we're using Excel for that.

So in that conversation, I think we've already fleshed the pieces part I would use to have the broader conversation. I think that's kind of a very basic example, but truly, we've done this sort of analysis for some of the largest banks in the world and some of the smallest water departments in the U.S., by way of example, and the logic is the same, which is: What is it that you do? Break those things down into categories, then talk about the assets required for those categories of operations, and then start exploring these requirements, the protection sustainment requirements. When you start addressing protection sustainment requirements for assets, then you quickly move to a discussion of the CIA triad that we know from cybersecurity-- confidentiality, integrity, and availability.

Sticking to those fundamentals, you'll develop a list of the things that are most important and the things that you're doing now to protect and sustain, and things in the future that you probably should consider doing to protect and sustain.

Bobbie Stempfley: And then we put them under crisis, right? Because that--

Matt Butkovic: Yes.

Bobbie Stempfley: Put them under additional stress, because that's then the other piece, that idea of identifying your assets and prioritizing the protection and sustainment of them is important, but then ensuring that you're doing that in a way that helps you prepare for the next stressor, not just enables you to think about what you would do in sort of a stressful situation. I think that becomes important when we think about organizational resilience, is how to shore up beforehand.

Matt Butkovic: Yeah, thank you. This is why capability and maturity models matter, because they're predictive. We don't want to know just what you're doing today kind of in a checklist mode, but what are those indicators of process and practice institutionalization that allow you to survive disruptive events. We won't know the total population of disruptive events. There's a universe of things that could happen, and lots of them we can't anticipate or even game out in a setting like this, but if you understand the fundamental resilience of your operations and assets, then the specific nature of that threat is less important.

So again, the more you know about institutionalization of practice and process, the more predictive it is, because things that are institutionalized, or acculturated, inculcated-- to use a bunch of terms we like to use in the academic setting-- the more survivable those things are. If there's something important we do in our Etsy enterprise and only Bobbie knows it, and then Bobbie is unavailable, she's incapacitated for some reason, or the information is unavailable because we lost the spreadsheet, we know them that we're unlikely then to meet our mission, we're unlikely to continue that operation.

And then basic example then plays through clearing and settlement for the national financial infrastructure. It's the same logic, which is: What are those things that are most important? What are the variables that affect them? What does it look like when they're impaired? And you just go through those calculations, understanding what the output will be, that allows you to then tune and find harmonization of practices and processes so that over time, if you apply this resilience mindset, resilience engineering way of working, you're finding efficiencies. You're finding maximum coverage for the controls and the practices, so you're not doing things as a one-off. So if you do these things in combination, you're left with a better ability to predict, you're doing them more efficiently, and you can worry a little less about the specific nature of the threat because you're contending with and preparing for a wider spectrum of threat actors.

Bobbie Stempfley: I think we've got time for one last question, and let's take this to the other extreme. So we're no longer a single microbusiness making something and selling it on Etsy, which has a nontrivial supply chain as well, right? You need a supply chain for the raw

materials, you need the distribution mechanism through the postal service or UPS or something. Now let's think about this in terms of a large organizational that's critical infrastructure in a region or heavily interconnected with sort of a deep supply chain concern that's there. I can see how all of these would scale and be applies and executed, but then how do you think about doing that with your partners? Because one part of I think organizational resilience-- and I think buried in the information and the people elements of assets-- are who our partners might be that enable us to execute whatever that sort of important mission is.

Matt Butkovic: That is absolutely an essential point to make, Bobbie, which is your external dependencies, as we call them, your reliance on those organizations and assets that are outside of your direct control is absolutely imperative, and this is getting more complex all the time. So you'd be hard-pressed to find an organization that doesn't use the cloud in some way, as an example. So I think the lines are blurring between assets you operate and assets someone else operates, in a functional sense. The cloud storage I rely on is seamless to me by design, but the way it's managed and the way it's secured is not seamless because I don't do it, right? So to your point, Bobbie, you have to think about this extrapolation of your requirements, the extrapolation of your needs as they're applied then in the third-parties on which you rely.

We have a body of work in external dependency management, supply chain management, at the SEI that attempts to address this. So it's an excellent point: You can't look at this in isolation. You also can't just assume it's only the supply chain, meaning raw materials and shipping of finished goods. Think about the public services you depend on. Potable water. Natural gas. Electrical power. Roads that reliably allow you to do conveyance between two places. These are all types of external dependencies. So I think your point is a really good one, which is we have to think expansively about this, but that doesn't mean confusing ourselves. We should start small and then let that radiate out. "Here are the things we do. Here are the people we touch that do them that aren't under our direct control," and then look at that comprehensively.

Bobbie Stempfley: Right. So I think there's this tension between preparing and really thinking about preparing, and responding in a crisis. When I think about resilience-- we have a question about which of those ways is more effective, and I think, in my experience, any kind of crisis management and success in crisis management is largely dependent upon how well you've prepared, and perhaps you didn't prepare for the exact terms of this crisis, but you are prepared for a set of things, you've practiced with a set of things, and you can then rely upon them in a crisis situation. When I think about resilience as a sort of planned and emergent property, it really only can emerge if you've done the basics, if you've done the legwork.

We have about a minute left here, and I just want to give you the chance to make any last comments, Matt, that you didn't get a chance to share.

Matt Butkovic: Two comments, Bobbie. First is the topic that you were just exploring. It's not an either/or, it's a both, right? You have to--

Bobbie Stempfley: Absolutely.

Matt Butkovic: You have to both plan and also-- you have to plan for contingency but also then ensure that you've addressed kind of standard controls. So don't look at it as an either/or. And I just wanted to thank you, Bobbie, for the opportunity this afternoon this talk about these things. We're living in extraordinary times. I truly believe that the folks that are watching this in our profession should take solace in the fact that the fundamentals are seeing us through. We can't take our eyes off the objective of ensuring that our organizations and our systems are resilient, and I look forward to future dialog on the topic.

Bobbie Stempfley: I think that's really important to recognize. We are success inasmuch as we are today because we have focused on building relationships between practitioners, building relationships inside organizations, and really help to focus on those four key assets types, that people, facilities, technology, and information, and I think that's really an important element.

How we evolve in this world across that spectrum of what is the crisis and execute I think will largely depend on how much we rely on and mature our processes and our linkages between the business outcomes and those things that support that business outcome, so I really look forward to that. I think this is an important discussion and one that will continue on over the course of the next-- the weeks and months ahead.

I also want to thank everyone for attending today. These webcasts are a great deal of fun and I hope you get a lot out of them. I really hope you get to join us for our next webcast, which is the 15th of July, and its topic will getting insight, not just oversight, into the progress of contractors using Agile, and Suz Miller will be that webcast host. Everybody that attended will be emailed the registration link, and thank you so much for joining today.

Matt Butkovic: Thank you.