Title: Managing Disruptive Events: Demand for an Integrated Approach to Better Manage Risk Transcript

Part 1: Using Multiple Preparedness Plans Can Be Ineffective and Inefficient

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 principal researcher at CERT, working on operational resilience. I'm pleased to welcome back my colleague, Nader Mehravari. Nader is a member of CERT's Cyber Resilience Center.

And today, Nader and I will be discussing the second in his three-part series on principles and practice of operational resilience. Hopefully you got a chance to listen to Part 1. So in today's podcast we will be discussing better ways to deal with a range of disruptive events, and the factors and pressures that are driving organizations to adopt a more integrated approach, which Nader will discuss.

So, good to have you back on the podcast series, Nader, thanks.

Nader Mehravari: Hello Julia. It is really good to be back here to do the second part of the three-part series, where we have been discussing, as you said, concepts related to operational resilience.

Julia Allen: Great. So just to help listeners refresh, are there a few key points from your first podcast that you would like to recap, to set the stage for our conversation today?

Nader Mehravari: Sure. I think that's in fact a good idea. Last time during the first podcast, we started by talking about destructive events. And our discussion was very broad; broad in a sense that we talked about destructive events of all kinds, whether they were natural or manmade. Natural: like we talked about Hurricane Sandy. Manmade: we talked about an example of the nationwide failure of the power grid in India last summer.

Accidental or intentional: Intentional like terrorist bombings or cyber attacks. Small or large; physical or virtual: physical like explosions and shootings; virtual like data corruptions or even fraud.

We talked about some real examples that demonstrated that destructive events are becoming, let's say, more bothersome; not because there are more of them or not because they are occurring more frequently but because our risk environment is changing. It's rapidly expanding and therefore these destructive events are becoming more bothersome for our organizations.

And the question was in this ever expanding risk environment what should organizations do to deal with destructive events going forward? Because some of the traditional methods may no longer be effective.

Julia Allen: Right, and I also recall us discussing how very public -- with the way that news information is propagated almost in real time through the internet, the fact that an organization can make one misstep and it's very public, correct?

Nader Mehravari: Correct. And since our business environment is not very friendly these days--maybe 10, 15 years ago, businesses could get away with one or two mistakes. But these days many organizations fail after the first time when they take a misstep.

Julia Allen: So to continue our conversation from last time, and for our listeners' benefit, Nader's full presentation is available with the show notes. We're going to be talking about the middle part of the presentation.

The first thing I wanted to ask you Nader is in your tutorial you do a deeper dive now on again some additional recent examples of disruptive events where the organizations that were impacted had traditional solutions in place -- these more bounded, stove-piped approaches to dealing with disasters and crises.

And so I was hoping you could give a few more examples where some of these more traditional solutions might have worked. But probably more importantly for our conversation, places in which they started to break down.

Nader Mehravari: Yes that's a good question. Again, using real-life examples are probably the best way to demonstrate some of these issues. So if we quickly remind ourselves of what I refer to now these days, a triple disaster in 2011 in Japan, which was a combination of a major earthquake, followed by a tsunami, followed by a nuclear incident.

Clearly organizations in that part of the country executed their disaster recovery plans, their business continuity plans, their crisis management, crisis communication plans, etc.; and very traditional preparedness plans that many organizations in that part of the country are used to have and execute. And some were successful and some were not. It was a major, major event. In 2011, the same year that Japanese disaster occurred, there were a lot of very publicized cyber security attacks.

Maybe the most publicized one was when Sony Corporation's PlayStation network -- a very large and popular game network -- was breached and was affected. Clearly Sony Corporation executed their information security protection, their cyber protection, crisis communication plans. Again, a slew of preparedness plans -- that they had in place.

A recent major flooding in Thailand about a year ago caused a major disruption in, I have to say, global supply of computer hard drives. Because Thailand is now becoming a primary center for development and manufacturing hard drives, that caused a major disruption in the supply chain. And those companies who had put in place a supply chain contingency plan executed them, which is different from traditional disaster recovery business continuity plans.

Recently an employee of British Petroleum lost a laptop -- a laptop that contained records, including personal information about 10, 12, 13,000 individuals who had submitted claims for the BP spill a couple of years ago. That incident caused BP to execute their privacy breach incident plan, which is yet another preparedness plan that organizations have to put in place because of the changes in the privacy law.

So what we see is organizations, public and private, are being forced to continue developing a large collection of mostly independent and stovepipe preparedness plans. And every time something happens, they have to pull one off the shelf and execute it independently. And as the risk environment changes, these collections are becoming larger and therefore more expensive to maintain and manage.

And the more plans you have, there's a higher risk that you're not managing and upkeeping them, and there's therefore a higher risk that they're not executed properly. So that's one of the observations that are being made by subject matter experts about our current environments.

Julia Allen: Right, so you've given some great examples of all these moving parts; the emergence of new types of risks that are calling for yet another type of preparedness or continuity or response plan. And you started to describe a little bit about how this is becoming more and more difficult to manage.

So when an organization does have this approach to responding to disruptive events using multiple plans, can you say a little bit more about some of the challenges and what you've observed? How organizations are both struggling and maybe starting to migrate to a different way of thinking?

Nader Mehravari: At some level most of these plans are risk management activities. At that level, they all have a common mission. They're all trying to deal with risks that are being realized. And therefore if we do some coordination, some level of collaboration between these plans, one opportunity is that reduction or elimination of redundant activities.

So that's something that organizations are suffering from because it's a lot of time and effort and energy to keep all these plans up. If there are some coordination between these plans, then some of these redundant activities can be eliminated or reduced.

Julia Allen: Nader, what about some of the roles? It occurs to me that there's lots of different players. You've got different people, different roles being responsible for each of these plans. What do you see in terms of the emergence and addition of new roles to take on all these different plans?

Nader Mehravari: So traditionally, for example, disaster recovery plans in many organizations are under, say, the IT organizations or the organization's CIO whereas the business continuity plan is under management of maybe operations or manufacturing. So there's a lot of roles.

If an organization again looks at all of their plans, all of their preparedness plans, and determine that they want to introduce some level of integration or coordination, that type of action would allow an organization to have maybe a centralized role developed at maybe a higher level of the corporation that could have some ownership across all the plans, and therefore do connect the dots between different organizations, the people who own these plans, and reduce in future development of additional new kind of plans. So this enterprise-wide role to look at all the plans is something that would definitely help organizations become more efficient.

Part 2: Government and Market Demand; Increasing Standards

Julia Allen: I know in your tutorial you have a significant number of examples where you've observed in different market sectors a growing demand for the use of a more integrated approach. Could you share some of those examples with us today?

Nader Mehravari: Yes that's a really good question because so far we are talking about let's say observations and opinions from subject matter experts. And it's always good to see the other side of the coin; to see other people who are actually asking to do things differently; or other business cases that says, "Hey, we should consider to do things differently."

So here are some examples of places that I've noticed that there is a desire to do things in a more integrated fashion. In some observations from our federal government here in the United States, if we compare, for example, some of the latest versions of the White House's cyberspace policy document and compare it to maybe similar versions from four or five years ago, we'll definitely see a language change where the latest version of White House's cyber policy review document is asking stakeholders to consider dealing with and coming up with game changing technologies that have the potential to enhance not one thing but a collection of things -- security, liability, resilience -- all together. So you see a language change there that goes toward this concept of not developing plans for one risk but looking at all the operational risks at one time.

Another good example for me is when a government organization offers investment and research money for organizations to develop something new. If we look at the Department of Defense's priorities for 2013 through 2017 -- which was issued last year -- in that document the Secretary of Defense has listed seven areas that DoD is planning to invest additional resources.

One of those areas is actually titled Engineering Resilient Systems. So this is a new area that's been added to that list of priorities to Department of Defense. So that's another indication that our federal government is thinking in that direction.

It's always good to get data from other countries. So a good example is the direction that the United Kingdom folks are taking. If we look at their latest version of their cyber security strategy for the United Kingdom, we see a similar language change or desire that they are looking for a solution that is both safe and secure, and resilient at the same time.

The thing I like about their plan is, in fact, they have very explicitly have set aside a small portion of their investment budget for people to do work in these integration activities, which is a good sign. Another place to look at is our academic institutions. We should ask the question: “Are academic institutions changing what they are teaching their students?”

And if we look at some of our universities in the United States, I have seen new degree programs: Master of Science in Resilience Management, for example; or degrees in Disaster Resilience Leadership; or post-graduate degrees in resilience. So our academic institutions, who often develop new academic programs based on the needs of their stakeholders, are starting to begin teaching those type of skills.

Julia Allen: On those degree programs Nader, are you finding those are coming out of the more technical disciplines, like computer science and engineering? Or out of the policy or business administrative colleges? Or is there a mix?

Nader Mehravari: The ones that I have seen and have some familiarity with are either coming from traditional engineering schools and disciplines or from management and business schools.

Julia Allen: Okay.

Nader Mehravari: But then the other place to look at is the job market. I recently looked at some of the job advertisements in this area. And I've noticed that there are explicit job postings that they're looking for subject matter experts that have both, for example, information security and disaster recovery expertise. In fact I just saw one recently that says -- the title was: Cyber Security and Resilience subject matter expert. So I think the job market is a good indication too as to what the organizations are looking for.

Julia Allen: Great, great. Standards, laws, and regulations tend to lag what's going on in our respective marketplaces. But I know you've identified a growing number of standards and regulations that are also pushing us in this direction, that either now or very shortly organizations are going to have to demonstrate compliance with, depending on their respective markets.

So can you say a little bit about standards?

Nader Mehravari: So there's some good examples that indicate that both national and international standards, and some other regulations, are sort of catching up with this concept that doing information security, disaster recovery, and business continuity at the same time might be more efficient and effective.

So after the 9/11 incident, and after the 9/11 Commission issued their findings and recommendations, one of the recommendations was that -- to Congress -- was Congress shall establish a mechanism for private sector in this country to measure themselves, from a perspective of how prepared they are.

The reason for that recommendation in the 9/11 Commission was that they realized that 80% of the critical infrastructure in this country is owned and operated by private sector. And we have no mechanism to assess how prepared that 80% of the critical infrastructure is. So based on that, Congress actually did pass a law. That law designates Department of Homeland Security to be responsible to put in a program for private sector entities in this country to measure themselves.

DHS has done that. Their program is called PSPrep; it stands for Private Sector Preparedness. It's a voluntary program. And DHS identified several standards that private sector entities can use it to measure themselves. There is a set of program specifications, and people that they can be, go to, to be measured, etc.

The other interesting information about standards is it's now technical. It has to do with financial aspects of running our businesses. Firms like Standard & Poor's and Moody's and Fitch -- these are organizations who rate the financial instruments of our corporations.

They now include in their annual assessment of the financial instruments of companies aspects of enterprise risk management. And their definition of enterprise risk management includes things like disaster recovery and business continuity. So this is a recognition that financial number alone no longer tells the whole story and therefore our U.S. corporations need to worry about how to demonstrate to these rating organizations that they're prepared. One way to do that is to measure themselves against a standard. So our standards are becoming more important.

Julia Allen: Were there any others that you've noticed that you wanted to call out here? I notice, again in your tutorial, that even the ISO organization is getting involved in things like supply chain resilience.

Nader Mehravari: Right, so the disaster recovery and continuity professionals actually are excited because national and international organizations are paying attention to the subject. In fact, I had the pleasure of overseeing several students at Cornell University who did a study of a number of standards in this area over the last 20 years.

And there is a drastic change in 2005/2006, going forward, that the number of standards coming from international organizations, such as ISO and other country-based organizations that issue standards, the number of standards dealing with preparedness planning has quadrupled since 2005/2006. So that's another indication that enterprises need to pay attention to the standards.

Julia Allen: Excellent, excellent. Well this has been a great additional increment Nader to move this dialog along in terms of what's driving us, moving from traditional approaches to a more integrated approach, and where some of both the market and the standards demands are coming from and how they're pushing organizational leaders to think about this.

So I know we've said a little bit about what we're going to discuss in our last and final Part 3. Do you want to say a little bit more to preview Part 3?

Nader Mehravari: So if you look at Part 1 and Part 2, we've talked about what are the problems; what are the challenges; what has changed over the last 10, 15 years in this area; and who's asking for different ways of doing things.

So the next natural question that people should be asking is: “Okay, what are the good ways to do this? Are there proven ways to do things better? Or are there better ways to do this integration of different preparedness planning activities?” So naturally our next session, we'll talk about some proven techniques; some cornerstones to be able to do operational resilience in better ways; and some examples of who have successfully done some of this work.

Julia Allen: Great teaser, Nader -- thank you. So to bring our podcast today to a close, do you have some additional places where our listeners can learn more on the subject?

Nader Mehravari: So some of the stuff that we've been talking about are based on a tutorial that I recently gave at an IEEE Homeland Security Conference. So that material is available at the website. And then if our listeners go to the SEI CERT Resilience Management website, there are quite a bit of material there that will be of use.

And then if they have not listened to the first part of this three-part series, that's another resource. And then, of Course, naturally they should come back and listen to the third part.

Julia Allen: Great Nader. Well again, I thank so very much for your time and your preparation today and for all of the great examples. Thank you so much.

Nader Mehravari: You're welcome; look forward to the third part.