Managing Disruptive Events: Making the Case for Operational Resilience
Transcript

Part 1: Traditional Approaches Insufficient: Surprises from Hurricane Sandy

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. Today, I'm very pleased to welcome my colleague, Nader Mehravari. Nader is a member of CERT's Cyber Resilience Center.

And today, Nader and I will be discussing the first in a three-part series that we'll be recording on principles and practice of operational resilience. And this series is based on Nader's extensive experience in applying operational resilience in a number of organizations. And also these conversations reflect a presentation that Nader gave at the IEEE Conference on Technologies for Homeland Security in November of 2012. And we'll provide a link to his full presentation in the show notes.

By way of background, if you are unfamiliar with CERT's work in operational resilience and our CERT Resilience Management Model, we have posted a number of podcasts and webinars at both the CERT-RMM and the podcast website to provide some background for you.

So, with no further ado, welcome to the Podcast Series, Nader, glad to have you.

Nader Mehravari: Hello, Julia. Thanks for including me in this program. I'm delighted to be here and talk about a topic that is very close to my heart, operational resilience.

Julia Allen: Excellent. Well, this will be great and gives us lots of time to explore all the good content that you've developed.

So, to set the stage, it would be helpful if you could provide a few recent examples of the types of disruptive events that can really affect an organization's ability to be resilient. And by that, I mean -- and you'll obviously talk about this, as well -- to continue to provide critical services and business processes in the presence of some type of disruption or stress. So, a few examples would help set the stage, if you could be so kind.

Nader Mehravari: The most recent example was the Hurricane Sandy that affected United States just about a month ago. But almost every year recently, there's been one or two very major events that we'll never forget.

Like in 2010 was the Gulf of Mexico Deep Water Horizon oil spill event that we continue to remember. In 2011 was the devastating earthquake followed by tsunami and a nuclear incident in Japan. And just in January of 2012, we saw those horrified pictures of the sinking of the Costa Concordia cruise ship in coast of Italy. So every couple months we see on major event that will remain in our mind forever.

Julia Allen: Absolutely, and it seems that we keep having to relearn the lessons of the past every time one of those events occur. So, let's talk a little bit more about Hurricane Sandy. I know in your tutorial presentation you particularly point out some of the things that were expected but some of the things that were surprising in that event. So could you talk about that a little bit?

Nader Mehravari: So, Hurricane Sandy clearly was a very major storm that hit eastern United States. It was the largest from a size perspective. The wind diameter was the largest recorded in Atlantic region, about eleven hundred miles worth of wind diameter. So from that perspective, any strong hurricane, we expect things to happen. In a hurricane, there's always expectation of flooding. And there was flooding, major flooding. In fact, New York City had the highest ever water levels recorded. In any hurricane, there's expectation of wind damage. And there was a lot of that in Sandy.

Power loss is a typical after effect of any hurricane. And there was a lot of that in New York, New Jersey area. And we have learned that there is always a need for portable power generators. And this time, the Home Depot and other hardware suppliers were ready. There was a run on power generators but there was good supply of them.

At the same time, however, Sandy surprised us in a whole different set of ways. There was a major devastating fire in a neighborhood in Queens, New York right in the middle of the hurricane that destroyed over a hundred residences in that neighborhood. A major fire in the middle of a hurricane is sort of surprising.

Julia Allen: Right, you wouldn't expect with all that rain and all that flooding that fire would be an issue, right?

Nader Mehravari: Right. And, since people were not expecting a fire, the first responders who deal with the fire were other places doing other things.

Sandy caused a very strange weather pattern, which caused a blizzard in West Virginia on its way up to New York. A blizzard in the middle of a hurricane is -- it's unexpected. They were not ready for it. And there were some very interesting pictures from Seaside Heights in New Jersey that if you looked at them, they looked like there was a sandstorm. There were four feet high sand dunes across the entire town.

So the lesson we learned from Sandy is that it doesn't matter how much historical data we have and how much prediction power we have in our computing equipment. Destructive events will continue to surprise us in ways that will disrupt our business operations. So the question is how do we deal with this concept of not always being able to predict exactly what's going to happen in a destructive event.

Julia Allen: Right, so we can, as you said, based on history, we can predict but there's a whole other set of unknowns and uncertainties. And the real question is, as you framed it, is how can we prepare for the unexpected, prepare for the unknown, correct?

Nader Mehravari: Yes.

Part 2: Traditional Approaches Too Stovepiped; Not Scalable

Julia Allen: Okay so, let's talk a little bit about -- I mean obviously there's a huge body of knowledge around business continuity, disaster recovery, crisis management, emergency preparedness. There are all kinds of traditional disciplines that have stood the test of time, that allow organizations to protect and sustain themselves when such events occur.

And yet, in our work, the work that we do together, we are really finding that an operational resilience perspective can be more effective. So can you say a little bit about the traditional disciplines and this kind of evolution or migration in your thinking to operational resilience?

Nader Mehravari: So you're absolutely correct. Destructive events are not something new. They've been happening forever. And communities and businesses have developed over the years emergency management plans, disaster recovery plans. Our federal agencies have continuity of operation plans that they spend resources developing and then putting in place. And all of those plans have to be developed, managed, updated. That takes time and effort.

However, over the last ten, fifteen years, those traditional preparedness plans, such as disaster recovery plans and continuity of operation plans, are no longer sufficient. And organizations are forced into developing a slew of other preparedness plans to protect and sustain their operations.

Some of the examples are, over the last seven or eight years, there's been a lot of attention on dealing with pandemic plans -- having protection plans in case there is a flu pandemic. So that's a new class of preparedness plans that are being developed. Recently, our organizations are dealing with more sophisticated contingency plans that deal with people related issues -- how to deal with the workforce not being available after an incident. And by workforce, I include in there executives the decision makers.

So, workforce continuity planning is now becoming another one of these individual siloed plans that organizations spend time and energy developing. Our globalization of manufacturing has made the supply chain a lot more sensitive to disruption. And therefore companies or organizations are putting in place supply chain continuity plans to protect and sustain their supply chain.

So we're coming to the mode of organizations being forced to -- needing to develop a large number of such plans. And developing in silos are not efficient. Developing in silos are costly because they cause duplication of effort. So the question is, is there a better way to go around, go about developing these modern and needed preparedness plans.

So a fundamental cornerstone in the concept of operational resilience is to somehow introduce some level of coordination, some level of integration across all preparedness plans, whether they are protection or sustainment activities -- so they don't look like individual silos. That, I think, is a critical aspects of operational resilience that we are looking at and trying to determine what's the best way for organizations to achieve it.

Julia Allen: Right, because it seems to me, listening to you talk -- and I was unaware of some of the new areas that some of this planning is having to occur. There's the planning. There's the exercise and test. But then when something bad happens, obviously there's the execution. And you've got all these moving parts trying to coordinate a reasonable response, and protect the enterprise, and its customers, and all the assets that are involved.

So, it seems to me that, as you said, developing in silos, how do you -- in the face of an event -- how do you orchestrate all of those moving parts?

Nader Mehravari: Right. So if you continue our traditions, you would need a lot more resources than any organization can afford. Execution of each one of these plans individually and by their own is no longer feasible for anyone.

Part 3: Operational Resilience to Better Deal with Fast, Public, Global Disruptions

Julia Allen: So can you say a little bit more about what you mean by operational resilience and why you think this is so promising as a shift or an expansion of perspective?

Nader Mehravari: The concept itself is very simple. What can organizations, public or private, small or large, families or communities can do? So if there is a destructive event that causes unavailability of certain resources or assets, how can those organizations continue operating,

continue developing products, continue doing their business operations under stress while the event continues or while preparedness plans are being executed to recover?\

So that's the overall concept of operational resilience. It's not just dealing with individual consequences. It's not just dealing with individual assets. It's a big picture look at an organization that says, "Ok, what do you have to do, what are all the good things you should be doing on a regular basis so you are a resilient organization?

Julia Allen: Got it. Got it. Thank you. So why do you think -- I mean you've laid the groundwork here in terms of what's happening in our world that is causing organizations to pay increasing attention.

But can you say a little bit about why senior executives, in particular, in the private and public sectors, why this is elevating on their radar screen as something that they need to be investing in?

Nader Mehravari: So, our today's environment such that the moment a disruptive event takes place, it's very quickly and very highly publicized. And therefore, it is practically impossible for our organizations, our businesses to ignore it. And whether the effect on them is small or large, they have to respond to the fact that the event is taking place and they have to do something about it.

I mean just looking at the past ten months, just looking at the events in 2012, there is a long list of major and minor destructive events that became major headlines across the world, ranging from other tropical storms other than Sandy -- like tropical storm Isaac that affected the Republican Party national convention, which was delayed for a couple days.

Or just a few weeks earlier than that, typhoon Haikui that affected evacuation of about a million people in Mainland China. Or all the disruptive events we hear on a daily basis on the news dealing with information technology and cybersecurity.

Just within June, July, August of 2012, we had a major incident at LinkedIn, a popular social network, that affected six and half million users' passwords. Two weeks later, Yahoo was affected by release of close to half a million passwords. And then just a week later in July, Twitter was down for a good portion of a day because two of the data centers failed at the same time. And then later in July, there was a major electric grid failure in India that caused close to, I think, six hundred million people to be without power.

So events are happening quite often. And maybe not more frequently but they're very public. And therefore, businesses have to respond to it and therefore executives are paying a lot more attention to it.

Julia Allen: Right, well as you said, with the news cycle and the way information is instantly released, and customers can be very fickle and end up doing an instant migration to what they perceive to be a safer space, it can have -- a lack of due diligence in this area can have immediate effect on your bottom line, right?

Nader Mehravari: Right, and organizations asking the question, "Hey, are there more disruptive events happening" I mean that's a good question to ask. But it may not be the best question to ask. In fact, there is no consistent set of data that one can use to say, "Hey, there are more disruptive events happening."

But a better question to ask is, "Even if the number of disruptive events are not increasing, is something else has changed that causing disruptions to be more important or more critical?" And the answer to that question is definitely yes.

What has changed over the last ten, fifteen years is the fact that our risk environment, our global risk environment, has changed and has worsened. And here's some examples. Clearly, globalization of our economy has resulted in our organizations' dependency on resources all over the world. So when there's a small disruption in a particular part of the world, if that affects a supply chain, it may affect a large number of companies here in the United States. That's an increased risk in our manufacturing environment.

Julia Allen: Mm-hmm.

Nader Mehravari: Our business operations have become a lot more complex, both in public sector and in private sector. And therefore, smallest disruptions and disturbances causes the entire business process to fail.

We don't have to have more disruptions but even small disturbances causes a much bigger effect. Pervasive use of technology -- we all now fully dependent on our mobile devices and our laptops. And that now, when there are small disturbances, there are more effects of it.

So the question to ask is how should organizations deal with this expanding and worsening global risk environment? And the answer might be that the traditional techniques that we all have been using may not work anymore.

Julia Allen: Right, it also occurs to me as I'm listening to you speak, we talked about instant media attention. But this whole phenomenon as brought on by the use of technologies around speed, the fact that so much of this is happening faster and sometimes is harder to detect in advance sufficiently to mitigate the effects.

And so you're dealing with the aftermath. So speed, it occurs to me, is a significant contributor to what is changing and shifting, and thus the need for more automation support, right, in terms of the response and the recovery? Are you seeing that as well?

Nader Mehravari: Right, we no longer can depend on quote unquote “manual operations” to recover from incidents because that just takes too long. And our business environment, in general, is a lot less friendly. That is, if there was something they could get away with ten years ago, we no longer can get away with it.

And therefore, recovery procedures have to be much faster, almost immediate, to the point that maybe the customers or media won't even notice that an organization was affected by a destructive event. But they continue providing business.

So we have to remember a very important thing that today's business environment is very, very unfriendly to organizations, to the point that some of them may not get a second chance if they're not effective in dealing with that first major incident.

Julia Allen: Well, before we come to our close, Nader, could you just -- as I mentioned at the top of the podcast, this is going to be a three part series. Could you give just a short preview of what we might be talking about next so we can intrigue our listeners to come back for more of this conversation?

Nader Mehravari: So I have mentioned a lot of my observations. So I think it will be good for our listeners to also see some indications from other sources that will indicate that yes, there is a desire. There are people who are asking questions like, “What are the better ways to deal with disruptive events?”

So we can give our listeners some indications of what are other places, what are other organizations who are asking for better ways of doing this. And then, there are some concrete techniques and approaches that an organization can take to improve and measure their operational resilience. And that would be another interesting topic to discuss with our listeners.

Julia Allen: Excellent, those are great teasers. So can you provide, at this juncture, some additional places where our listeners can learn more about what we've been discussing?

Nader Mehravari: So as you mentioned at the beginning of our discussion, I was fortunate enough to be able to give a half-day tutorial on the subject at last month's IEEE Conference on Technologies for Homeland Security. So that material from that tutorial will be available to our listeners as part of the show notes.

And from a bigger picture perspective, if our listeners go to the CERT resilience management website, they'll come across a slew of material on that website. And then, by listening to part 2 and part 3 of this series, they actually will pick up additional information.

Julia Allen: Excellent. Well, I'm looking forward, Nader, to our continued conversation. And I thank you so very much for your time and preparation today.

Nader Mehravari: You're quite welcome. And thanks much for the opportunity.