Operational Resilience and Risk

Table of Contents

Operational Resilience -1 ................................................................................................................ 2
Operational Resilience -2 ................................................................................................................ 5
Operational Resilience and Risk ...................................................................................................... 6
Elements of Resilience ...................................................................................................................... 10
Notices .......................................................................................................................................... 12
Operational Resilience: The emergent property of an organization that can continue to carry out its mission in the presence of operational stress and disruption that does not exceed its limit.

[CERT-RMM]

Where does the stress and disruption come from?

**018 On operational resilience, what is resiliency? Well, think about a spring. You’ve got a spring. And you stretch it. And you let go of it. What happens? It snaps back to its original shape, right? What happens if you pull, pull, pull, pull. And you hear this doink. When you let go of the spring, what happens? It doesn’t go back, right? You’ve exceeded the resiliency of that spring. So, resilience, if you look at the physical world definition of resilience, it’s the ability of any material to be able return to its original shape after some type of stress, as long as that stress doesn’t exceed its tolerance or its limit.

Look at this from an operational or a business standpoint. So, now you have
operational resiliency. And this comes from the resiliency management model. But it's an emergent property meaning operational resilience is not something that you specifically do. By emergent property, we mean that it comes out of all the things that you do. So, you don't sit down and go I'm going to do operational resilience. And it's this step. And I'm going to do this. And we're going to be great. Operational resilience is a combination of all the things that you do as part of your organization.

So, it's an emergent property that allows an organization to continue to do business, regardless of what happens to it. So, you have this term of operational stress. So, it's your ability to continue doing your business despite operational stress, as long as that stress doesn't exceed your limit.

When the stress exceeds the limit, what happens? You have functions that break. Your servers are no longer able e-commerce. You have information that gets compromised and now you've got legal and regulatory issues that cause you fines. And now you've got to pay all those. And that shuts your business down. Whole chain of events there. But what we're getting at here is if you have operational resilience, you can survive the bumps in the road that happen as your business continues. And you can keep continuing-- or you can keep going down the road of operating your business provided that it doesn't exceed your resilience limit or whatever that point might be.
So, your goal behind risk management and all that is to increase your resiliency such that you can survive a denial of service attack. You can survive an intellectual property theft, or somebody pulling information out of your network. You can survive a fire in your data center. So, all of that is operational resilience. That's why you do risk management activities is to achieve that.

So, where does the stress and the disruption-- so the operational stress or the operational disruptions that affect this limit or cause you to be resilient, where does that come from? Where does that stress and disruption come from?

Student: Risk.

Chris Evans: Your risk, right?
Resilience: The physical property of a material when it can return to its original shape or position after deformation that does not exceed its elastic limit

Operational resilience: The emergent property of an organization that can continue to carry out its mission in the presence of operational stress and disruption that does not exceed its limit

Where does the stress and disruption come from? RISK

**019 So, if you look at your risk management process, what you're trying to do is figure out where can I be stressed. Where can disruptions come from? How can I mitigate those? How can I address those to increase my operational resilience so I can bounce as I go down the street and not be completely taken apart by whatever that is.
**Operational Resilience and Risk**

Operational resilience emerges from effective operational risk management.

Operational risk categories

- Actions of people
- Systems and technology failures
- Failed internal processes
- External events

**020** There are, like we said on the previous slide, there's operational resiliency is an emergent property. It's not something that you do in and of itself. It happens because of all the things you do holistically as an organization, primarily the risk management piece. If you can do risk management and be able to survive all of these various categories of bad stuff that can happen to you, you've got operational resilience.

How do you survive actions of people? Well, first you’d ask yourself what's bad here. What bad things could people do to me and my organization?

Student: Human error.
Chris Evans: Human error, right, accidents.

Student: Steal. Employees might steal something.

Chris Evans: Yep, stealing and theft, so malicious activity, hacking into things. The guy comes in and kicks the server or something like that.

Systems and technology failures, what could go wrong here? Power failures, right? Server just crashes. You have-- the operating system and the application that's running on it don't cooperate well with each other so that fails. So, you have problems here that you can address.

What about failed internal processes? This is actually an interesting one. It's probably one of the harder ones to actually address. What would failed internal process actually be? Well, look at your internal processes. What do you do as part of your business? How can that process break?

I'll give you an example here of a security process. There was a-- I did a pen test at an organization, very high secure facility. And part of their process of letting people in and out of the facility was they would issue a badge and PIN number. And when you got your badge and your PIN number, you would go to the mantrap area and you'd step into the booth. You'd swipe your badge, put in the PIN number. And if everything and agreed, and you were in the system, it would let you into the building.

Well, an example of a failed internal process here is the security system was dependent on a database. So, when a
person showed up at the receptionist’s desk and said I’m here to see so and so, please look in the system. I should be in there. And I’d like a badge, please. So, when the person showed up at the receptionist’s desk and said here’s my name. The receptionist would look in the system for your name. And if you were in the system, she would go I see your request for a visit has been approved. Here’s your badge. Here’s your PIN number. Go right through the mantrap over there and enter the facility.

Where this process breaks is the receptionist just looks at the system, right? There’s not point of contact—there’s no call to the person you’re visiting to make sure that you’re supposed to be there or anything else. So, if somebody has access to the system, in which case—this case, we did. The system was actually a database server that was accessible through the Internet. We could actually inject ourselves into the database, put a line in there that says Chris Evans. I’m from this organization. I’m visiting Bob Jones. And check the visit has been approved.

Well, did that go through the normal accepted security process? Well, no it didn’t because nobody approved the visit. Bob Jones never said Chris Evans is allowed to visit. It was me putting my own information into the database. And so, the receptionist just looks at the database and assumes that if it’s in the database, or in the system, he’s allowed to be there.

So, that’s a good example of a failed internal process. The process itself works great as long as you follow the rules. But
as soon as you start bending the rules or finding ways around it, you get these internal processes that just break.

External events, what’s an external event? A hurricane, a fire, a flood, a lightning strike, whatever, war, terrorism, act of god, there’s a whole bunch of external events. When you look at business continuity planning, historically, business continuity planning has been about this stuff, the external events. How do I survive a hurricane? How do I survive a fire? So, business continuity, traditionally, is all about this. And now start it seeing to move into the internal processes, the technology failures, the what could go wrong from a cyber perspective, and IT perspective. So, it’s starting to account for more and more things, not just the fire, flood, famine, and those types of events.
You should focus on all three; do not ignore one for the others.

**021 Elements of resilience, so there are three areas that you can focus on within your organization. You can worry about physical security. You can worry about IT operations. And you can worry about business continuity, generally. So, within this, if you look at what business continuity is concerned with, it's keeping the business up and running. If I'm concerned about IT operations, it's my servers need to be running. Applications need to be available, etc. And if I'm worried about security, I'm looking at things like physical security, cyber security, potentially, and those sorts of things.
With resilience, you can’t focus on one area or two out of these three. If you do, you’re not really resilient. Look at the cross between business continuity and operations. Where do those two functional areas cross? Well, they usually cross with things like continuity of operations, redundant servers, back up servers, keeping back up data and that sort of thing. So, if you've done this and this, these are the types of things you're addressing, continuity of operations, redundancy, but you've ignored any type of security aspects, right?

So, if you're doing business continuity crossed with security, you're really doing life and limb stuff here. Right, how do I respond to a fire? Or how do I preserve life in case of a flood or something like that.

If you're concerned about-- or if you're looking at just security or IT operations, now you're doing cyber security, information assurance, and those types of activities. But you can see if you look at just two out of the three. You're missing something.

So, you have to put all three of these functions together, security, IT operations, business continuity. You put all three of those together, and what you end up with in the center is resilience if you're addressing all three areas, security, continuity, and IT operations.
Notices

© 2014 Carnegie Mellon University

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This material was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. government purposes, the SEI recommends attendance to ensure proper understanding.

THE MATERIAL IS PROVIDED ON AN "AS IS" BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark owned by Carnegie Mellon University.