**130 We've talked about the technical-ness of collecting all of this information together and organizing it to hand to management, not the raw data, but the summarized report.

We need to know what management's going to do with this. And so their process is to decide. And in our risk management best practices, we need to understand how they're going to make their decisions.
Risk Management Best Practices

Business continuity concepts
Fault tolerance
Disaster recovery concepts

They're going to take a much larger approach to this looking at things like business continuity, disaster recovery, and fault tolerance for the organization. They're going to take a bigger view of this. The classic example that I see happening in the environment today is you do a risk assessment on the servers, and I do a risk assessment on all of the workstations. And I think these things are critical, those things are not critical. These are low. And there's a very different set of opinions that's going on there.

When we combine these two together, what we realize is that
we're underpowered in our computing facilities and that we actually need to have an economies of scale. We take this, and then we're still underpowered. But then we go to the next division and the next division that are over there. And we realized that all of us are underpowered as far as CPU utilization on an individual box's concern.

And management steps back from this entire thing and says, "You know what? We need a lot more resiliency than we have here. So, what we're going to do is we're going to put virtualization in place. We're going to create a private cloud. And instead of having servers multiply out, instead of workstations having to have more and more power, we're going to centralize those process-intense facilities into this cloud that we use here." So, the workstations will still be out there. But when they need the demand of lots and lots of drive space, and lots and lots of processing power, we'll shift that burden to a centralized infrastructure because all of the activities that we have are bursty.

This also has another effect on us, which it helps us in business continuity. And it helps us in disaster recovery.
**Business Impact Analysis (BIA)**

Purpose is to differentiate between critical (or the most time-sensitive) and non-critical functions of an organization and understand the impacts of an interruption

Activities

- Perform risk / threat analysis
  - Make recommendations on whether risks should be accepted, transferred through insurance, or mitigated
- Identify critical systems and components
- Determine critical business processes, dependencies, and priorities
  - Through questionnaires, workshops, interviews, hybrids
- Review legal, regulatory, and contractual obligations
- Understand third-party dependencies
- Understand management succession plan

**132 When we do business continuity, we change the way that we look at a risk assessment in one key area. Well, there’s two. One is business impact analysis looks at the risk assessment and really only cares about the time it takes to restore. I don’t care why the server is down. How long will it take to me get back up and running? And what is the cost when it’s not running?**

What I should do is I should create a resiliency methodology here so that I can actually absorb lots and lots of CPU demand. And so, that would go into virtualization.
When we do business impact analysis, again, we look at time as our enemy. We look at availability as our core function that we’re trying to achieve.

When we do risk managements we start looking at who’s actually doing it. And we start getting into the specific threat and vulnerabilities and actually addressing them. We don’t do that in business impact analysis. So, we do a risk assessment, but it’s form a different standpoint. We look for the critical components to a particular business process. And we find the failures in those. We find out that we need redundancy for this particular process that we have in house.

Now, we can generate that redundancy in house by putting in more servers and hiring more people. Or we could generate that redundancy or resiliency by making it so that when we fail, we fail over to a secondary site or that we fail over to a cloud if we need to.

Now, most of your business impact analysis is driven, or your business continuity planning and disaster recovery planning is driven by regulatory bodies. You can use the concept of making sure that the organization is resilient so that when your competitors fail that you’re there to scoop up customers. And that might be a way to get more budget at this point because you know in a market, you’re going to act just like your competitors. If you act
differently and better, you can be there when that particular competitor fails.

You also have to realize that in business impact analysis, we look to the externalities, the requirements that we have where we might rely on a certain vendor outside of our organization to make us whole, to complete the transaction. If you're building cars, and you're assembling those cars, one of the key components in that is tires because you get tires from somewhere else. You don't have the tire facility here. You get those tires from another location. So, now you're dependent upon that facility.

Suppose that facility is a union shop and those union workers decide to strike? That strike in that industry costs you the ability to produce cars. You could ask yourself from a business impact analysis, how long do strikes normally last in that particular environment?

And you say, "Well, okay the longest strike that's ever been has been thirty days." Okay, what we want do is we want to have an inventory of thirty-one days' worth of tires. And we'll continually refresh that. So, we'll build up inventories here to make sure that if there is any constituent--if there are any components out there that could cause us problems that we have a buffer here. We could also switch to another non-union shop to actually acquire tires from another location. But that could be costly in our relationships.
Removing Single Points of Failure

In the network
In IT personnel
In dependencies

**Single points of failure** are “choke points” in the network where a fault in a single component causes some level of system failure. Not always “equipment” problems...

**133 One of the things that we’re trying to do in business impact analysis is identify single points of failure. And since we’re mostly on the technology side of things, we look for it in our IT resources, in our personnel, and any kind of dependencies that we have.

The most expensive thing and the most difficult to replace in single points of failure is an administrator that knows everything, and everybody else has to go to that person. So, we try to do cross-training for that person so that we make sure that there is no reliance on that person in case there’s catastrophic illness for them.
Single points of failure are the pieces within the organization where if that goes, the business ceases to flow. And so, we look for those. We either create a redundancy where somebody else can help us with it or a resiliency, a stronger person if you will.

**Business Continuity Planning and Testing**

**Business Continuity Planning and Testing**

Plans to ensure that critical business operations may resume in the event of failure or interruption of services

Should include

- Notification, escalation, and communications plans
- Logistics required
- Documentation development

Periodic testing of the plans include

- Developing test objectives
- Evaluating the test
- Developing recommendations to improve the response and recovery plans
- Implementing a follow-up process to ensure implementation of recommendations

**134 When we do business continuity planning and testing, in the planning stages of it we look at how we can get economies of scale and bring a whole bunch of things together. So, when we look at the test that we create for this, what we do is we say, "Okay, this really**
should include notification and escalation." In our testing facilities, what we do is we look at how all the other components of the organization interact.

Once we do this testing, and we do this periodic testing plan and put it in place, we need to find out from our testing what we forgot to do. And that's really what the testing does. This is the only time that, without a major cost to the organization, we can figure out what our potential failures are and fix them. One of the things that causes problems in business continuity planning is the staleness of the plan. And so, we need to keep on updating that plan over and over and over again.
Risk Assessment

Assess the environment for risks, evaluating each risk as to its likelihood of occurring and the cost of the damage it would cause if it did occur.

Assess the cost of various countermeasures for each risk.

Assess the current mitigation strategies to determine their adequacy in relation to the identified threats.

Prioritize and compare risks with possible losses.

**135 Now, we could use the outputs of risk assessments in our business continuity plan. Remember the idea is to look at all those risk to our organizations. But how could we help support business continuity and disaster recovery? Well, what we could do is we could start focusing in on those things that cause availability failures.

We look at the environment for risk. Is there a possibility of flooding? Is there a possibility of hurricanes, tornadoes, hailstorms? Take all those environmental conditions into play and say, "Is there a risk of these things?" So, now instead of our threat being something man made,
now we’re talking about Mother Nature coming after us. We'll decide and prioritize those risks with the possible losses and include that in our business impact assessment.

Continuity of Operations

Continuity of Operations

Procedures and guidance to sustain an organization’s essential functions at an alternate site for up to 30 days

- Determine which services or assets are most critical to maintain availability

**136 What we're really trying to achieve in a business continuity plan is continuity of operations. For those who are in the military, we talk about a COOP, continuity of operations plan, which is exactly the same as business continuity and disaster recovery mashed together. In our continuity of operations, we're trying to make sure that the organization continues.
Now, here's the trick. In continuity of operations, we don't have to run at a one hundred percent efficiency. What we need to do is we need to limp along to satisfy the customers' demand.

When we look at the training business, the requirement is that the instructor show up on time, be able to talk and articulate, and convey the information. So, if the instructor got a cough, what kind of control could we put in place so that the instructor could keep on teaching? Well, we could give him a cough drop. It will suppress the cough. It will stop the interruptions in class. But we know the instructor's going to go a little slower and a little quieter. They're not going to move around as much. But we'll still take that amount of training over the possibility of not training at all.

Now, in a perfect world, what we would do is we would have a stand-by instructor standing there. He's right there. Okay, come on. Go over and step in. And that instructor steps in and says, "Okay, we'll keep on going." But as we know in most businesses, what we have to do is we have to-- it costs us way too much money to do some activity like that. So, now what we do is we put some sort of controls in place to make the instructor more resilient.

What things can we do to make the instructor more resilient? Well, every time he talks, he can wet down his vocal chords so that they last for the entire five days. When he leaves and
goes back to the hotel room, we make sure that he takes a cab so that he doesn't get hit. We make sure that the instructor takes their vitamins every single day, washes their hands a lot, doesn't shake hands with people so that they don't get a cold and doesn't eat off of the buffet.

When you have a single point of failure, you try to increase the resiliency of that particular single point. Or you create redundancy.

**Disaster Recovery**

Disaster Recovery

Ensure the timely restoration of business operations if significant disruption occurs

Activated in the event of major system disruptions with long-term effects
along. We go a little bit slower. In disaster recovery, we say we've stopped. Operations have ceased. There is no training.

What will we do in this case? Well, we could go to a second instructor. We could postpone the class. We could do something else or lose the money.

In disaster recovery, what we tend to do is we tend to say that the resiliency and the redundancy methods did not work. So, therefore we'll take drastic actions to still achieve the objective and to get back up into training.

Disaster recovery says that we have stopped and that our resiliency methodologies have failed. And we're going to do something else.

When we-- let's get serious here and talk about this from an enterprise standpoint. When we talk about disaster recovery, what we say is we tried to fail over to our secondary site, and that did not work. There is no secondary site. So, what we're going to do is we're going to pick up the phone and call the person that gave us our original secondary site. We're going to call him up and they're going to say, "Well, I can't help you, but I've got a buddy across town where you can go where the facilities aren't exactly perfect, but they'll still work."

Because of that existing relationship, because of those existing plans, we
know that the steps to be taken here are going to be the same steps that we take over there. But they're going to be adjusted because the backup tapes don't quite work the same way. Or the servers don't have the same CPU utilization.

So, in disaster recovery we say we made these plans. These steps won't work as planned. But we'll use them as the basis for that plan that we have to fake at that point.

**IT Contingency Planning**

**IT Contingency Planning**

Cyber Incident Response Plan

- Provides procedures for mitigating and correcting a cyber attack, such as a virus, worm, or Trojan horse
- Addresses mitigation and isolation of affected systems, cleanup, and minimizing loss of information

Information System Contingency Plan (ISCP)

- Provides procedures and capabilities for recovering an information system
- Addresses single information system recovery at the current or alternate location

**138 When we talk about information technology contingency planning, we look for some of the**
reasons why it happened. Like in a cyber incident response plan, we're making this based on all the different possible effects that can happen to the organization.

So, in our cyber incident response plans we may say, "Okay. Well when the I Love You broke out, everybody's going to stay and work and help us. But it's not going to be forever." What we try to do in cyber incident response, by the way, is minimize the damage to the rest of the organization.

So, a friend of mine at a very large organization, when Heartbleed kicked out, their organization used a lot of remote access. At the exact same time this is when Windows XP was going end of life. So, what they said was, "We're going to turn over all the machines from XP to version 8.1." So, when it went end of life, they were also battling Heartbleed. All the remote workstations that were supposed to be out there, a lot of those were coming back at that point. And people were sending in their workstations to get them upgraded and even get new equipment at that point.

So, I'm sure you've heard the term alligators, lake, and where the water is rising to. That was the case for them. It was definitely lots of alligators, lots of water. And it was still rising.

And what they said was, "Our incident response plan for a cyber
event of this magnitude requires that we shutdown portions of our operation." And that meant all of their remote access for a third of their workforce was nullified. It happened to work pretty well for them because about-- of that third, about half of those people were going to be out of work anyway for a week because they had sent their laptops back. But the other half, the early adopters, said, "No, we want to work." And they'd have to bring in their resources to the location.

They did not have sufficient parking for them because so many people came into the facility. And they did not have sufficient desk and resources for them. So, they had to co-op some other areas of the organization.

It happened to be that this organization has some very large open facilities where they went and rented tables and chairs, and stood up wireless access points very, very quickly and got them to work. It took one extra day. So, in a cyber incident response plan you have to contend with the users within that. And that was one of the problems that they actually had addressed in theirs, what would they do when everybody came to work at the same time.

Now, when you look at information system contingency plans, this is recovery for the information systems themselves. One of the things that you have to address in there is what happens if this is a single point. What
happens if it’s your only active directory authenticator? What happens if it’s your only security administrator? How are you going to deal with that? Usually, how we deal with that, by the way, is we look for those external resources that we can outsource to.

Succession Plan

**Succession Plan**

Who will run the company if the CEO and CFO are attending a conference together and a natural disaster occurs at their location?

- Difficult for senior leaders to consider, but an important planning factor

Should clearly identify succession of responsibilities, allowing for those identified to be trained to the higher level of responsibility.

**139 Now, the military’s very good at this. But corporate America is not. They have-- usually they have one person with the keys to the kingdom on many different things. And that’s it. If that person goes, then they have a real struggle and a real problem.
When we deal with succession planning, we should have the cross-training in place. But also there should be a clear chain of command to know who’s next. This works very well in military facilities. This does not work very well in commercial entities.

**Tabletop Exercises**

**Tabletop Exercises**

Common way to test continuity or recovery plans

Involved parties come together to step through a scenario to discern weaknesses in the plan

Makes participants more comfortable with plans

When the tabletop exercise is complete, any lessons learned or plan shortfalls can be addressed

**140 The way we test for this is we go through a table top exercise. That's exactly what I did with that group of people was the table top exercise, figuring out what was wrong with the plan without actually going to the server. And we can do those exercises. But in the tabletop**
what we’re saying is, “Can we put all the pieces of the plan together? Does this make everybody comfortable with knowing that they may not be in charge, but they know that somebody else knows the information or where to find that information?” Now, this helps us address any kind of failures in the plan, any kind of shortfalls in the plan.

Notices

© 2015 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.