Critical Assets and Ops - Identifying

Table of Contents

Gather Information ........................................................................................................................................ 2
Valuing Assets ................................................................................................................................................. 4
Business Objectives -1 .................................................................................................................................. 6
Business Objectives -2 ................................................................................................................................ 11
Notices .......................................................................................................................................................... 16
**003 How do you determine what is critical to your business or to your organization? How do you know what assets you have and how do you know whether those assets are critical or not? Any ideas?

Student: You ask.

Chris Evans: You ask, right? Interviews, workshops, research, surveys. And what you're trying to do is understand that one, you as an individual probably don't have complete insight into everything that your organization does. You don't know all the pieces and parts that go into the processes that you do but you as the person running the risk management
effort, you have the ability to reach into senior management, process owners or business area owners, and even in the trenches network administrators, security personnel and do interviews, workshops, surveys, to find out what's important to you, so "C.E.O., what's important to you as a business" He's going to have a set of things. "Okay, Business Process Lead number one? What's important to you?" And she'll have a set of assets and processes and functions that are important to her. "Okay, Network Security Administrator, what's important to you?" and you'll get a whole bunch of ideas there. Basically what you want to do when you're searching for asset information is you want to start off with the question "What keeps you up at night?" So to the C.E.O., "What concerns you about the business? What keeps you awake at night?" Or "What wakes you up at four o'clock in the morning going 'I have to do something about this.'". What is that? And so you can use these basic techniques for soliciting that information from people within your organization.
Valuing Assets

Business value of resources must be assigned.

- The decision-making process will be **flawed** without **proper assignment** of value to resources.

- **Valuation**
  - Consider variables such as technical complexity, control procedures in place, and financial loss

- **Judgmental valuation**
  - A decision made based upon business knowledge, executive management directives, historical perspectives, business goals, and environmental factors

- Driven by **business objectives**
  - If it “breaks”, how bad could it be?

**004 How do you value an asset? What’s the value of a server? Is it what you paid for it? There is information on that server, right? So what’s the value of that information? If you’ve already integrated it into your network, what are the costs associated with replacing that server? So there’s a decision making process here that you have to consider the value of the assets when you’re going through risk management because it’s imperative that you understand what’s critical, what’s not critical, and also what’s really important. Well that value is based on a couple of different things. So there’s typical value such as the price that I paid for it, but there might be other issues that are like technical complexity, the financial impact...
of this thing going away, so there's some type of valuation associated with that asset. There's a judgmental valuation. This is opinionated, right?

So out of all the chairs that are in this room, which one is the most important? Is one of these chairs-- maybe this one is a little less rickety than the other one. Maybe that one has got a better armrest on it. Maybe the C.E.O. sits in that chair every single time and therefore that's the most important one. What we're getting at here is judgmental valuation. I think that one is most important because that's my opinion of it. Doesn't necessarily mean that that's costs more or costs less than anything else, but it's a judgmental business decision based on what I know of all the chairs in this room, what I think, and what I think is most important to me as a business. So that's judgmental valuation.

Value can also be driven by business objectives so I need all these chairs in the front row of the room, but I don't need any of the other chairs in the back of the room. So these are the most important chairs to me because these are the ones that I'm going to come in and sit down on. Well that's a business decision based on what's most important to me. If this chair breaks, how does that impact me? I have to go an extra three feet to sit in that chair. That's unbearable. I can't do that. So I need these chairs. So I have a business objective that says this is my set of chairs. These are important to me, and if these are gone I'm in trouble. So you can base your valuation of something based on impact or outcome to your business if those assets go away.
Identify areas that are important to your organization.

- Reputation and customer confidence
- Productivity
- Health and safety
- Maintaining customers
- Avoiding fines and legal penalties
- Financial stability or growth
- Political influence
- Ability to compete

Based on senior management’s view of the business goals and environment

Then…how would you describe “BAD” (aka “IMPACT”)?

**005 So business objective. These are areas that are important to your business. And they are things that you must consider or the things that you consider your business to be successful. So what’s important to your business? Well you might find that reputation and customer confidence are important to your business. The fact that you are productive and you are meeting hourly goals or something like that. That’s important to your business. Health and safety of your employees or your customers or the people you provide service to. Maybe maintaining customers, making sure that your customers are happy so they don’t leave you to go to some competitor.
Maybe you think that avoiding fines or regulatory oversight is important to you as an organization.

So all of these things up here are examples of what you would do or what you would do in order to be considered successful as a business or things that you would want to meet. Business objectives usually come from senior management. This will be the Chief Executive or the C suite team out there thinking that what do I need to do as a business to be successful? So these are business goals. The next step once you identify what’s important to your business, you start thinking about okay, how bad can it be? What’s the impact to my business if I can’t maintain customers? If I can’t have continual growth? What’s the impact to my business if my health and safety of my employees is affected? So what you’re doing here is you’re trying to understand what’s important to the business, and then what could happen to my business holistically if I can’t do those particular things? So let’s take a look at an example here.

Remember that we have Princess Pizza Company here and we decided that we’ve got a couple of different functions within the organization. We make pizzas and we deliver pizzas and somewhere in here we have some type of order system that tracks orders from customers and sends that to the making pizza people and also sends the address to the delivering pizza part of the business. So the question to you then is what would our business objectives be? So we kind of already identified those for the strategy already up here. We said growth, reputation, making
lots and lots of money. Maybe how do we deal with competitors or something like that? Those could be considered business objectives, but let’s take a look at this particular area right here, making pizza and to a lesser extent the ordering system area. In order for us to consider making pizza a success or this particular business function to be successful, what do they need to do or what are some of the business objectives for making pizza? So I think one of them might be that we keep up with demand. Right? So in order for our making pizza function to be successful, when I get an order, I have to make it and I have to be able to keep up with the number of orders. What other sorts of things would be an objective here?

Student: Finding an official way to get our supplies and our ingredients.

Chris Evans: Okay. So suppliers. Maybe constant access for lack of a better word, right? So making sure that when I put a pepperoni pizza together I have the pepperoni to put on it. What else?

Student: Employees.

Chris Evans: What about employees?

Student: Hiring employees, keeping employees or retaining them.

Chris Evans: Okay. So staffing. I have to be able to hire and retain staff. What else would we do that would make us successful as a business?
Student: Figure out what your customers want.

Chris Evans: Okay. Yep, so make tasty pizza because if the customers don't want to buy it, well, I could sell them a piece of cardboard and they probably wouldn't appreciate that too much. I think another one in here is make profit and this is kind of a broad reaching one here but the idea that we're tied into the payment card system here so there's a linkage between making pizzas and the ordering system. If the ordering system breaks or any aspect of it breaks, my ability to make pizza isn't really affected. I can still make pizzas but I just can't take payments for them or I'm not getting orders or something like that. So I think making money might be another one too.

Student: What's the difference between strategy and objective?

Chris Evans: Strategy here?

Student: Yeah.

Chris Evans: So the way this is defined is there's different tiers of risk management or different focuses for risk management. The top tier, tier one focuses on the strategy of the organization. Tier two will focus on specific functions within the organization, and tier three might focus on particular information assets so what we're saying here is that there are different risk management processes going on. At the strategy level the risk management would be focused on growth and reputation and that sort of thing. Here what we're saying is risk management might be focused on these particular
things that we just came up with. So these are our objectives for the making pizza function.

Student: Some of them are duplicates, quite similar.

Chris Evans: Yep, they will be. Different focus areas though right or different scoping. So where we are talking about I think you said tasty pizza here is very similar to what’s here, but this is doing it from a corporate perspective as opposed to here we are in the trenches actually making the pizza. So at this level they would be concerned more with say customers from all ten branches of the store or something like that whereas this function would be maybe just at that store. So we'll come back to this in a second.

So that’s business objectives, areas that are important to our organization. So the last bullet point up here, we're talking about what is bad, what is the impact to us if something regarding our business objective breaks?
Business Objectives -2

Be specific

EXAMPLE: “Service Availability”

- **High**  Service is irrevocably destroyed or damaged.
- **Medium**  Service is disrupted for more than 2 hours, and some effort and expense is required to recover.
- **Low**  Service is minimally affected < 2 hours; little or no effort or expense is required to recover.

**006 Again this can be a qualitative statement meaning we have high impact, medium impact, or low impact. Or you could be quantitative about it and say my impact is five or three or whatever the case may be. You get to choose. But what we said here is we took an example and we said okay, what’s the impact to our business objectives? What, well so we arbitrarily picked "Service Availability". This would be an example of our e-commerce site has to be up and running otherwise we have negative effect to the business. So what we said was service availability. If the service is irrevocably destroyed or damaged, we have a high impact. Meaning if our e-commerce
system goes away we can't make money. We can't take orders we're in big trouble from a business objective perspective.

Medium impact might be that if the service is disrupted for two hours and we have to spend some resources and some expense to put it back online that might be a medium impact to us. But if our service, you know if our e-commerce service goes down for less than two hours, that's really a low impact on that because maybe we can stack up our orders or we just put up a Webpage that says "I'm sorry, system down for maintenance". But we know that our customers will come back to us after two hours to place their order. So when you're thinking about impacts to your business objectives, there's usually a component of time that you can use to graduate low, medium, high impact or there's cost, time, and resources associated with putting all that back together.

So if we go back to our example here. I want to be able to get two pieces of paper on at the same time. So if we say that let's pick one of these objectives and let's say our objective then is to, that's business objective, not what you might think it stands for. Our business objective here is to keep up with demand. So I need to be able to make pizzas as the orders come in. If we try to quantify what would be a high impact, what would cause a high impact to our business, what would be a medium impact, what would be a low impact, how would you quantify high impact to the business for making pizzas? And we'll give you an example to get us started here. If I said that I can't make pizzas for two hours or more, that would
result in a high impact to our organization. Now it doesn't really matter why we can't make pizzas, but what this is saying is that if for whatever reason I can't make pizza for more than two hours, I'm in big trouble when it comes to my business. Because think about the impact of this, right? So the next step in this process you’re going to be thinking about impacts. But what’s the impact of not being able to make pizza for two hours?

Student: You lose money.

Chris Evans: I lose money. Right so this, my ability to make dollars is affected. My customers are impacted by that. If I don’t make money, I can’t pay my staff or my suppliers as the case may be so this pretty much has broad-reaching impact on why this would be a bad thing. So what would be, let’s pick a low, the opposite extreme here. What would be a low impact to the business? So maybe something associated with time, right? Maybe I can’t make pizzas for 15 minutes, 10 minutes. Is that a big deal? Generally no because what is if you look at your average pizza customer, when you call and order a pizza what do they tell you? Thirty to forty-five minutes and no guarantees that it’s actually going to get there on time or anything like that, right? Well they account for small little operational stresses that might mean that they can’t deliver the pizza in 30 minutes or less. So a low impact might be something like a short term loss or inability.

So here low impact to the organization would be I can’t make pizzas for 15 minutes. I didn’t say no impact because
that would definitely impact our ability. Now we’ve got orders stacked up and out of ten customers, you could probably count on one of them being really pissed off at the fact that they’re not going to get their pizza in forty-five 45. Now I’m going to have to take care of that and whatever the case may be. So what would be a medium impact here? Any guesses?

Student: I don’t have peppers. Half of the orders come in and ask for peppers.

Chris Evans: Okay so ingredient-based or lack of. Right? Okay that’s a good example of a medium impact because now the customers who ordered peppers are going to be pissed off that they can’t get their pizza with peppers. But maybe if I give them ten percent off, they’ll come back. What is that ten percent off that I just offered them? Think about the whole risk mitigation process. One of my risks is customers get upset that they don’t have peppers on their pizza. I’ve offered them ten percent off their next pizza or something like that. What is that? That’ a control or a mitigation strategy. So my risk is people who are upset. My control is I’ll give them ten percent off and that will make them happy again, so a preview of things to come. We’ll get there. But if we want to continue down this route of inability to make pizza maybe it’s 30-plus minutes during the peak demand.

So what this might say is if I can’t make pizzas for 30 minutes under peak demand, I’m going to get upset customers or pizza orders are going to backup or something like that. So you could look at this with the two examples we just gave here, you could look at this from an ability
to make pizza or you could look at it from an ability to deliver pizza that the customer wants. Either way, what you’re trying to quantify here is impact so that when you have an impact to the business. So when you have an actual threat or a scenario that you come up with, you can look at this and go okay, my pizza supplier or my pizza sauce supplier is going to be ten minutes late today. What kind of impact does that have on my business? Well probably somewhere down here on the low. Whereas opposed to my oven blew up today and I have no way of making pizzas. That is a high impact. So this is giving you a way to look at particular risks and say is this high, medium, low, and a way to prioritize your impacts.
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.