Threat Scenarios

Table of Contents

Threat Scenarios

**020 Instructor: Right now I'd like to talk to you about threat scenarios.

Threat Scenarios

Critical asset or process

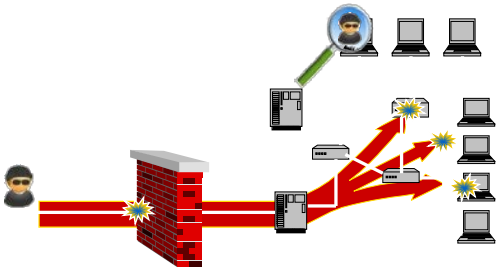
+ Valid threat

+ Real vulnerability

+ Controls or lack of controls

+ Impact on the business

Threat Scenario



Next step, analyze risks and figure out what plans you need.

- So far, we assumed a general likelihood of occurring; in risk analysis we consider how likely it is that something will happen.

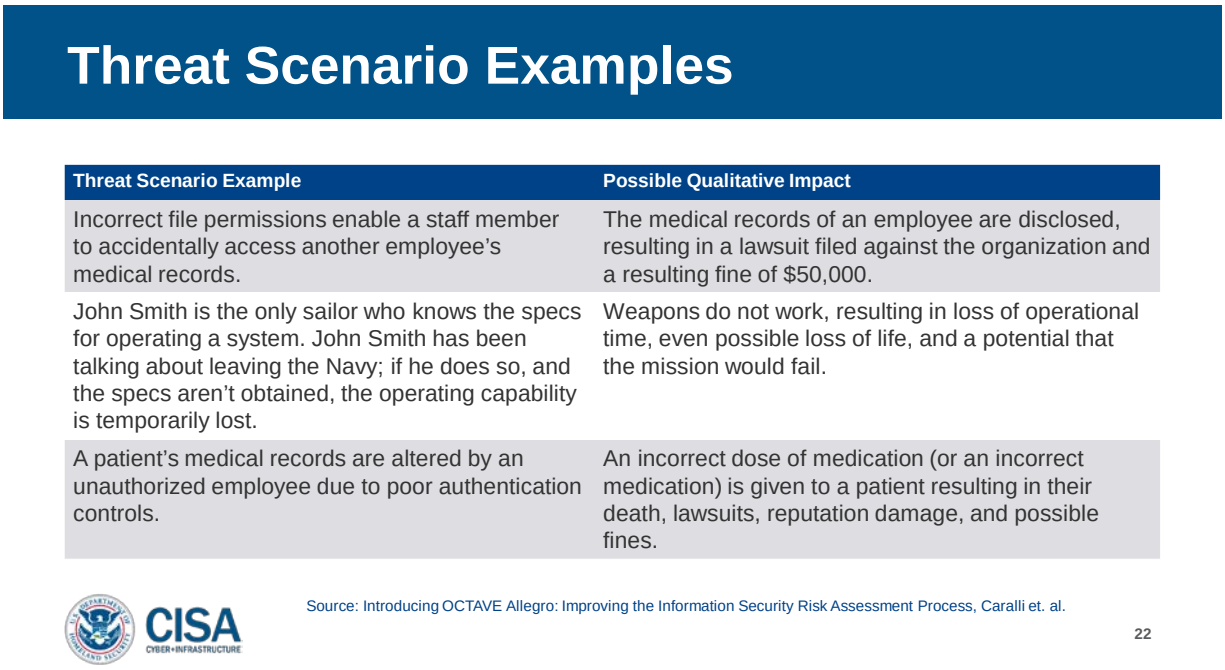
CISA CYBER+INFRASTRUCTURE

**021 So we understand that risk is comprised of uncertainty that is related to vulnerabilities that are in a system, and there's threats that are going to act upon those vulnerabilities to create some kind of impact for the enterprise, and when we think about this we might want to go back and think about what are the scenarios or what are the things, the sequence of events that may take place, that would result in a risk coming to fruition?

So we want to think about this and decompose it in a--a means that we can understand what the threat is and we, by the way, we want to make sure that's a valid threat, meaning it's a threat that would really want to impart impact to the system. We also have to have a vulnerability that is known in the

system for this scenario. I guess what we could do is if not a real vulnerability you could synthetically invent one, but the question there would be what are you trying to get out of the threat scenario? You could also develop what kind of controls are existing in your system to build out that scenario and use it as a tool to identify what controls you don't necessarily have, and most importantly you want to think about how that threat scenario results into an impact on the business, because at the end of the day what you really want to do is understand the priority or how you want to think about that risk among all others in terms of responding to it.

So what we want to do is understand how likely this could happen as well.



**022 Now, here are some examples of threats. Threat scenarios. I like to focus on the second one, and we have a sailor, and he's the only person on the ship who knows how to operate a system or maybe understand specifications for that system, and he's talking about leaving the Navy. Now, this could be a problem, because if he's about the only one on that ship that knows how to operate that system, it's going to take time for that ship to maybe get yet another expert like Mr. Smith back on the ship. So if he leaves, those specifications or whatever it is that he's walking away with, we're going to lose that for a period of time. We may lose some operating capability or maybe some piece of resilience that we really rely upon.

Now, you could have a qualitative impact there. Whatever the system

is that that person works on that they have expertise in, you're looking at the possibility of losing the utility of that system. We talked too, the fact that this could be more than just an impact. You could have other outcomes that may be interdependent with other risks.

So for example, suppose I have a risk related to this weapons system now that Mr. Smith has left the Navy, and I go to a new theater where that weapons system is required. There could be a cascade of risks now where actually if I don't have that weapons system I could fail a mission, and now you're starting to talk about how these risks, not only are they dependent upon each other, but they may actually start amalgamating into bigger problems for your fleet.

Likelihood Determination

- To derive an overall likelihood rating, indicating the probability that a potential vulnerability may be exploited within the construct of the associated threat environment, the following governing factors must be considered.
  - Threat-source motivation and capability
  - Nature of the vulnerability
  - Existence and effectiveness of current controls
- The likelihood a potential vulnerability could be exploited by a given threat-source can be described as high, medium, or low.

CISA CYBER+INFRASTRUCTURE

23

**023 That's how you want a scenario to play out, or at least how you want to think about it. You also want to talk about how you're going to think about the likelihood of that certain scenario taking place. Now, this can be an art and not as much as it is a science at times. You want to think about some elements such as what's the motivation of that threat source? What does that threat actor want to do? How capable are they? You also want to think about the vulnerabilities in the system that you're really addressing. Are they common? Have they been addressed? You want to think about the controls that you already have in place too. How effective are they?

Ultimately the threat scenario would hopefully point to controls that you don't have in place, so that way you

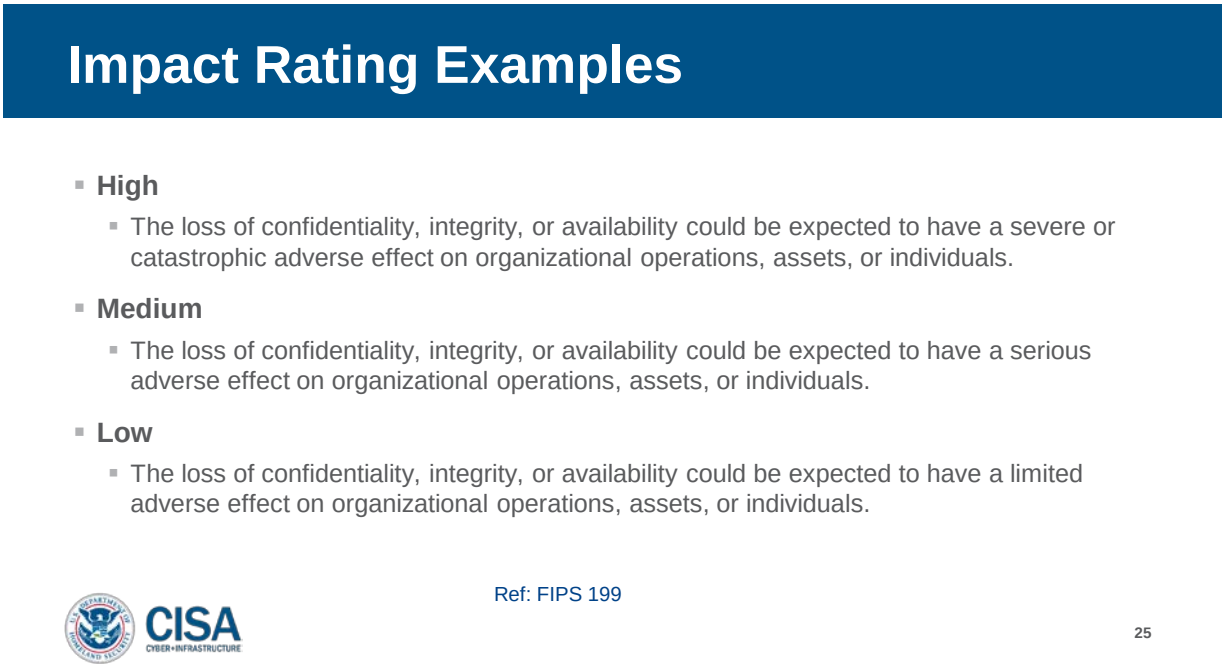
know where you need to commit resources on addressing that particular threat.

Likelihood Rating Examples

**024 Now, we've talked about a little bit, about how threats can be characterized in qualitative terms, high, medium and low. In this particular case, NIST SP 800-30 provides you with some definitions. Now, they're very general, but I like how they kind of break out the idea that at high, you have a highly motivated source, like we just talked about, the threat motivation, and you also talked about the capability, and now you're talking about, like, is it a state actor or is it some kind of script kitty in a basement somewhere? All the way down to the low level where maybe you have a threat actor who has no motivation to penetrate your system and maybe they have limited to no capability.

So qualitatively you can look at it that way. Another way we could look at it is in terms of how we're going to rate the impacts to the system.

Impact Rating Examples



**025 And we can think about this in terms of high, medium and low as well. We can have severe or catastrophic adverse effects on a system such that maybe we can't recover it ever again. We may also have it on the other side of the spectrum where we do have an impact but it's so low that we can clearly keep operating even if we have trouble with it.

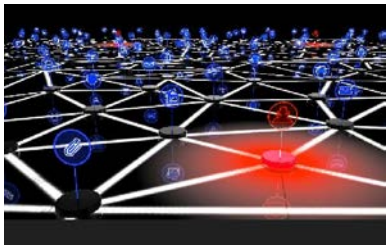
I'd recommend to go see FIPS 199 if you have any additional questions about how you might want to go about using these impact ratings.

Risk Calculation

- Risk can be measured ***quantitatively*** or ***qualitatively***.
  - Risk is given values so management can decide what to do about the risk.
  - The risk assessment should include
    - Criticality of the lost function
    - Duration the loss will persist
    - Tangible and intangible impact on the organization

What is the damage?

Physical inventory
Loss of data
Ability to conduct business
Good will and reputation
Customers and investors



CISA CYBER+INFRASTRUCTURE

26

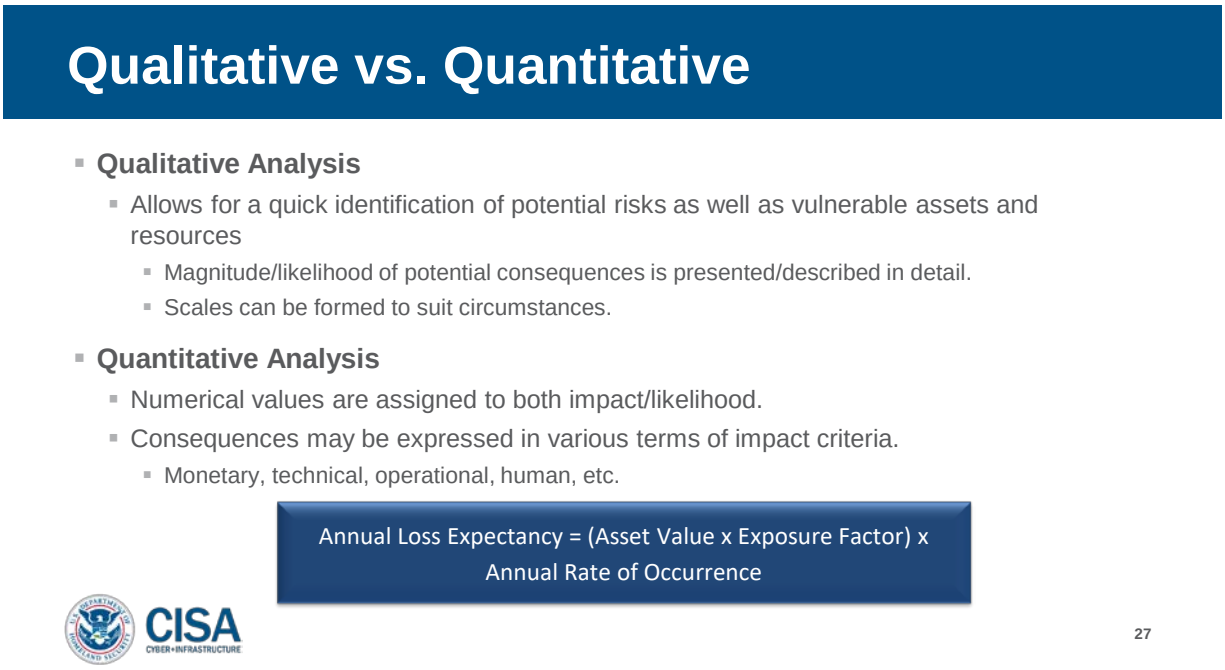
**026 Once you have these understood, you want to start thinking about how to quantify them so that we can bring it down to a risk calculation. Remember, the goal here is that we want to have the risk at least assigned some sort of index or some kind of quantitative or qualitative measure, that we can prioritize them and understand how to commit resources to them.

So what we really want to know is what assets are impacted in the organization? And dial that back to what function did we lose? What critical element have we lost that we can't conduct business as we want to? What objectives can we not accomplish? How long will we not be able to do that? Will it persist for an indefinite period of time? We'll have to take action to overcome it, and we

want to think about not just the tangible actions or impacts, I'm sorry, the tangible impacts to the organization. We want to think about intangible impacts as well.

A classic example for intangible would be reputation. Now, clearly, we all want to have a good reputation, especially with our customers, because we want return visits from said customers. If our reputation is damaged in a way that is challenging to measure, how is it that we're going to know if customers are going to be willing to come back or not? It's really hard to wrap our hands around some of these things, so you could rely upon maybe surveys, customer surveys, marketing surveys, but in the end of the day you really need to understand how that pain is felt on the organization.

Think about what is the damage that you're feeling? Is it the fact that you've lost data? Maybe you can't conduct business. By the way, that data's going to have some value to it. Maybe it's the fact that you can't conduct business because you've lost that data. Maybe your reputation is damaged such that you'll never get a return customer.



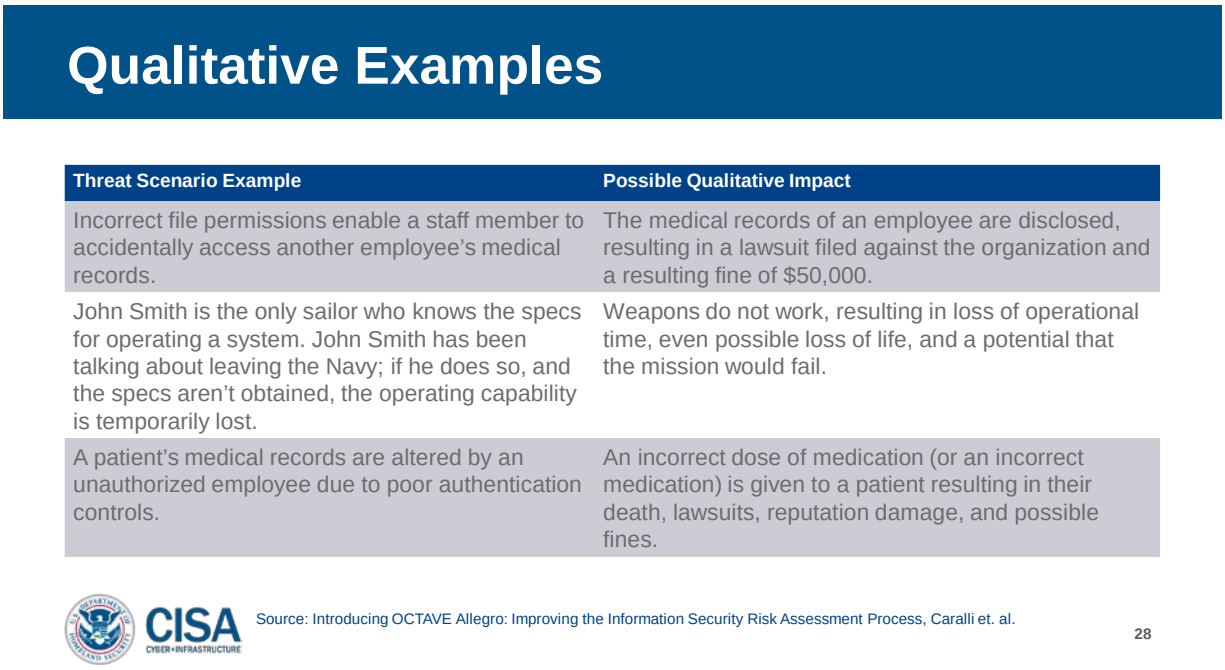
**027 So let's go a step further in comparing that qualitative verse quantitative nature. So for qualitative analysis, what we really want to do is we have a high-level assessment of what's going on and we understand that we have potential risks, and we're really trying to just get our hands wrapped around the magnitude, the order of magnitude for that particular impact, let's say, of the consequence.

You can do some basic scales here. I've showed you already the high, medium and low that NIST provided. We could also think about this though in a more quantitative sense. We want to think about what kind of numerical values we can assign to each of these levels of high, medium and low. It's one thing to say that a risk is going to have an adverse

impact on our organization, but what's that really mean? How do we feel that pain? Is it a hundred dollars? Is it a million dollars? Is it more?

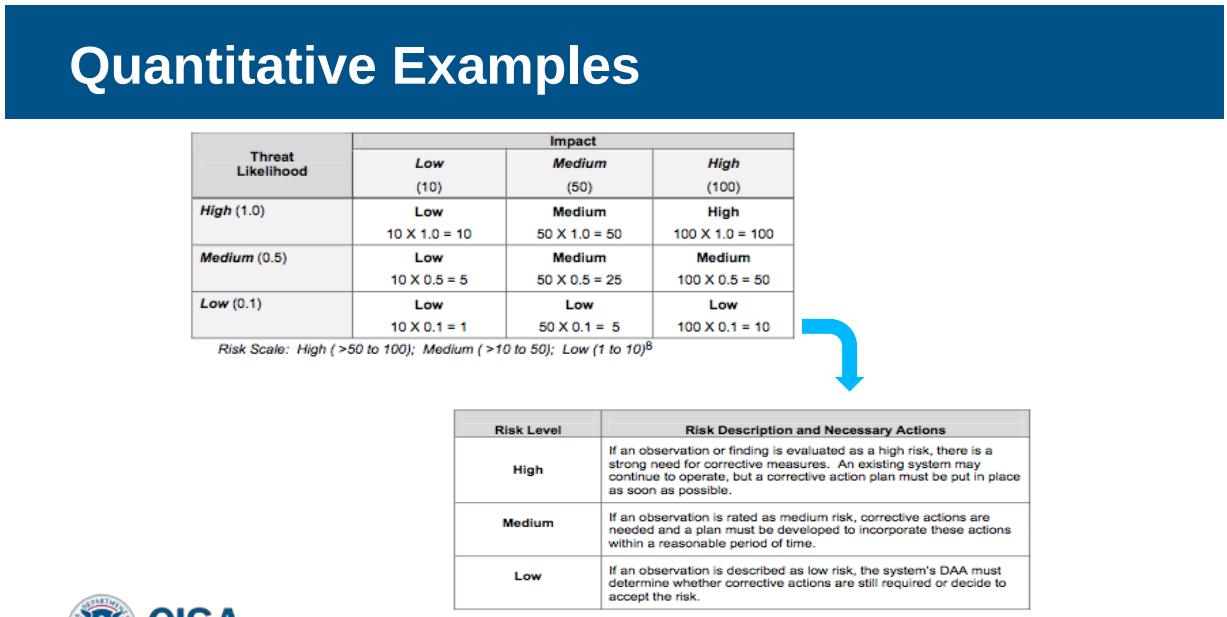
So we also have to think about what units we're going to quantify this in. I just mentioned money, but it may not necessarily be money. Maybe it's people. Maybe it's time. So we want to think about this and with respect to, once again, how you feel that pain. We can think about this too in terms of annual loss expectancy. It's a simple measurement, but the fact that you can read it and say it's simple, it's not necessarily as easy as it looks to get the values within the equation.

But let's talk about it for a second. Let's see what we can do here. Before we've talked about trying to measure the value of any given asset. You can maybe dial that back to the idea of, "What's the critical service that's delivered from said asset, and what kind of money am I making with it?" What's the value? I can think about the exposure factor. So this would be a number typically between 0 and 1. It's a decimal, and it's the likelihood that it is going to suffer some sort of detriment. I may also think about an annual rate of occurrence. So classically I may think about something that occurs every so often. If that event happens once a year, my annual rate occurrence would be once per year, and I can calculate this, what my expected loss would be, on an annual basis.



**028 So going back, I've given you already this example of qualitative examples. I wanted to show you one more time and get a general sense of the idea that largely it's words.

Quantitative Examples

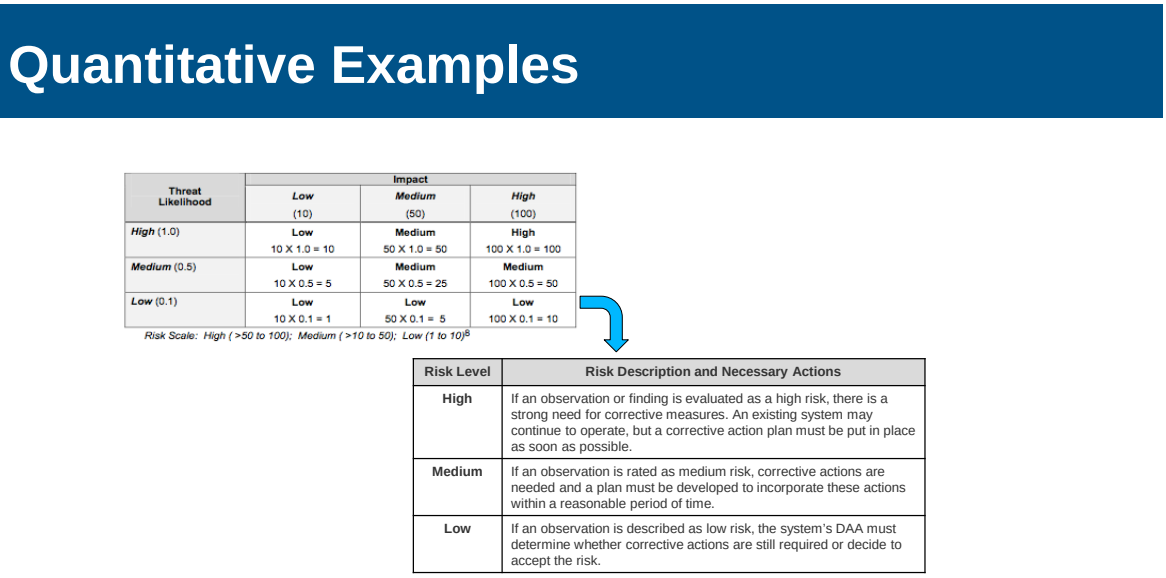


**029 Now, what I want to do is I want to turn that into a quantitative example, and I can think about this in all varieties and manners. Some things I want to mention about quantitative examples here, one is a lot of times when we establish some kind of appetite statement or some kind of index, it's very organizationally dependent. It depends on what your people think. It depends on the value of your assets.

For example, in this particular case, this appetite is talking about threat likelihood, and it, if it's high, the person has said that, "Hey, it's a hundred percent to me. It's 1.0. If it's medium, 50 percent; low, 10 percent," and if I go across, I can frame my low, medium, high impacts in terms of 10, 50, 100. For the sake

of argument for today, let's just say that's dollars. I can actually set up a matrix with this now, and if I said that I have a high likelihood to lose a high impact of a hundred dollars, well, my index for that is a hundred dollars. That's my expected monetary value for the risk.

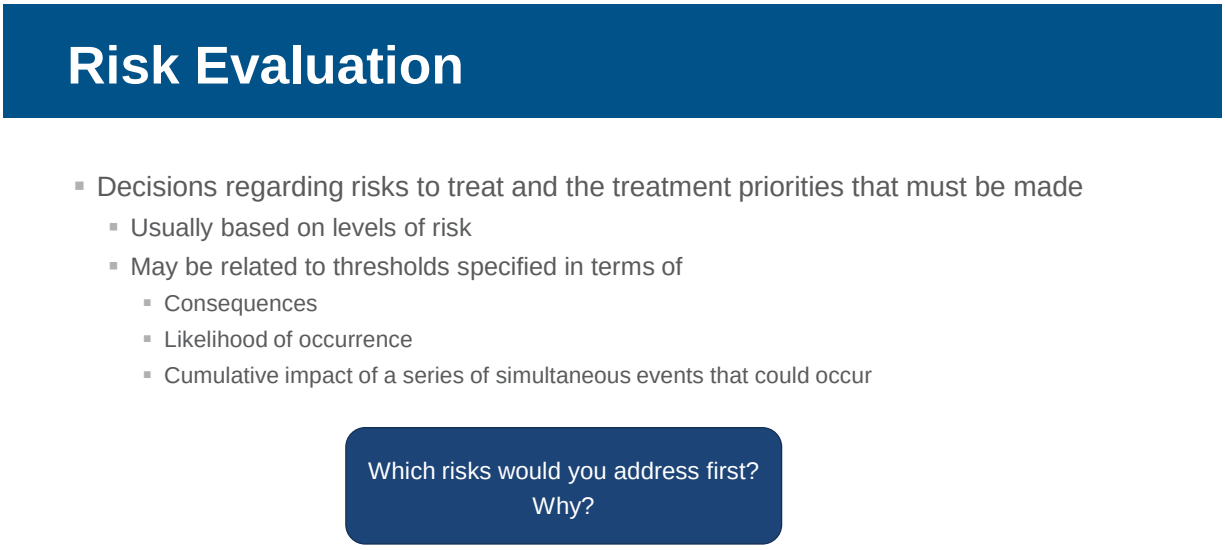
Quantitative Examples



**030 I could also think about this in terms of putting it in terms of a risk description in actions that need to be taken with respect to alleviating those risks, and the examples are given here. For example, if I have a high-risk level, I know that if I know that that risk is going to happen, that there's going to be a need for me to have some kind of corrective measure in place, without question, and without doubt. So no doubt, it's telling me that I absolutely have to invest resources, especially to that

risk, before I go start looking at other risks that may rate or rank lower.

Risk Evaluation



**031 This is what we call risk evaluation. We're making risk-based decisions to treat those risks in a prioritized manner such that we're allocating resources and that we are getting the risks addressed and we're getting our confidence in those risks coming to fruition brought down to a level that's acceptable to the organization. If that's the case, what we also want to think about with these risks are the thresholds or the specified limits that we're not willing to violate in an organization if a risk were to come to fruition.

So I ask you, if you go through your risk evaluation, you want to think about how do you know which risks

you're going to address first? Why would you do it?

Notices

Notices

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM18-0098