Risk and Impact Analysis

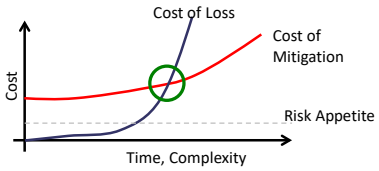
Table of Contents

Risk and Impact Analysis

**001 Instructor: Today we're going to talk a little bit about risk and impact analysis.

Determining Risks

- **Risk is an inherent part of business.**
  - Not all risks can be eliminated.
  - Every organization has a level of risk that it will **accept.**
    - Risk Appetite
- To determine the reasonable level of acceptable risk
  - Determine an optimal point where cost of loss intersects with cost of mitigation
    - Your risk appetite may not be sufficient by itself.



CISA CYBER+INFRASTRUCTURE

2

**002 Remember what we're trying to do here is we're trying to identify uncertainties in the business. It's an inherent part of what we're doing in any activity that we have. You're going to have risk there, so you really need to get your hands around it and understand it, and you really need to kind of get to the base and find out what you're really willing to accept, because as you're addressing this risk, you're going to have potential losses in the organization, but you're going to spend some money on the other side to prevent those losses from occurring, whether it's you getting ahead of the risk so that you can reduce the likelihood maybe of the risk taking place, or maybe eliminating a threat, or maybe you're investing money so that after the risk has happened, you have some sort of disaster recovery and business

continuity plan in place so that way you can keep your organization operating.

There's a sweet spot that you have to find there, and that sweet spot can be translated in terms of a risk appetite. It's basically what the organization is absolutely willing to tolerate in terms of risk, and you have to operate to that risk appetite to make sure that you have an acceptable level of risk in your organization and you're not spending too much money on the other side. In a sense, you don't want to build a million-dollar fence around a stack of pennies, is what we're saying.

Types of Risk

Types of Risk

- **Aggregate Risk**
  - Exists when a particular threat affects a large number of minor vulnerabilities and the combined affect has a significant impact
- **Inherent Risk**
  - Results with the risk linked to a particular activity itself
- **Control Risk**
  - Comes from a failure of the controls to properly mitigate risk
- **Residual Risk**
  - Remains after the controls have been applied to mitigate risk

CISA CYBER+INFRASTRUCTURE

3

**003 So let's review real quick the types of risks, because we're going to go through how we're going to actually assess these., and I may use these terms from time to time.

For example, an aggregate risk is when I have a variety of risks that may add up to having a more significant impact in the organization. This could be characterized as something like the death-by-a-thousand-cuts kind of analogy. So as an example for this, maybe we have a phishing email that may pose a very minor threat to the organization, but it goes to thousands of people in the organization, each of them being minor vulnerabilities in a sense as individuals, but in the end, if they all were to take root, if everybody was to open them up, it would have a significant impact on the organization.

Once again, Let's go over the idea of inherent risk. No matter what we do, the activities we participate in, even on a daily basis, no matter how regular they are, they're going to have risk in them. Think about this in terms of a production operation where I'm working in a facility. There are safety risks working around heavy equipment, things like that, where people could get injured. That would be inherent to what we're doing.

Now, suppose I want to actually set up maybe some safety features or controls in that plan to prevent issues from happening-- to prevent injuries, if you will. Some of these controls may actually inhibit the person from doing their work as fast as they can.

For example, suppose I have a punch press and the punch press actually

pulls the operator's hands out of the way before the punch press was to come down. There's going to be a time element there for that operator to have their hands come up every time for that safety feature. Well, here we have a control risk. You're actually imparting risk on the organization that you may have a detriment to the productively time. So that would be a risk around control.

And then you also have this idea that no matter how much I work, no matter what I do to plan around it, there's potential that that operator still could get injured. This is considered residual risk. No matter how much money I invest into it, there's always this potential for some risk to come to fruition.

Performing Risk Assessments

- Businesses organizations **should have a regular process** to perform risk assessments at
  - Organizational level
  - System level
  - Application level
- **Risk assessments help to identify threats, vulnerabilities, and the possible outcomes** currently residing in the enterprise.
  - Vulnerability testing
  - Penetration testing
    - Overt
    - Covert

- ISO 27005 and NIST SP 800-30 provide guidance for conducting risk assessments.

CISA CYBER+INFRASTRUCTURE

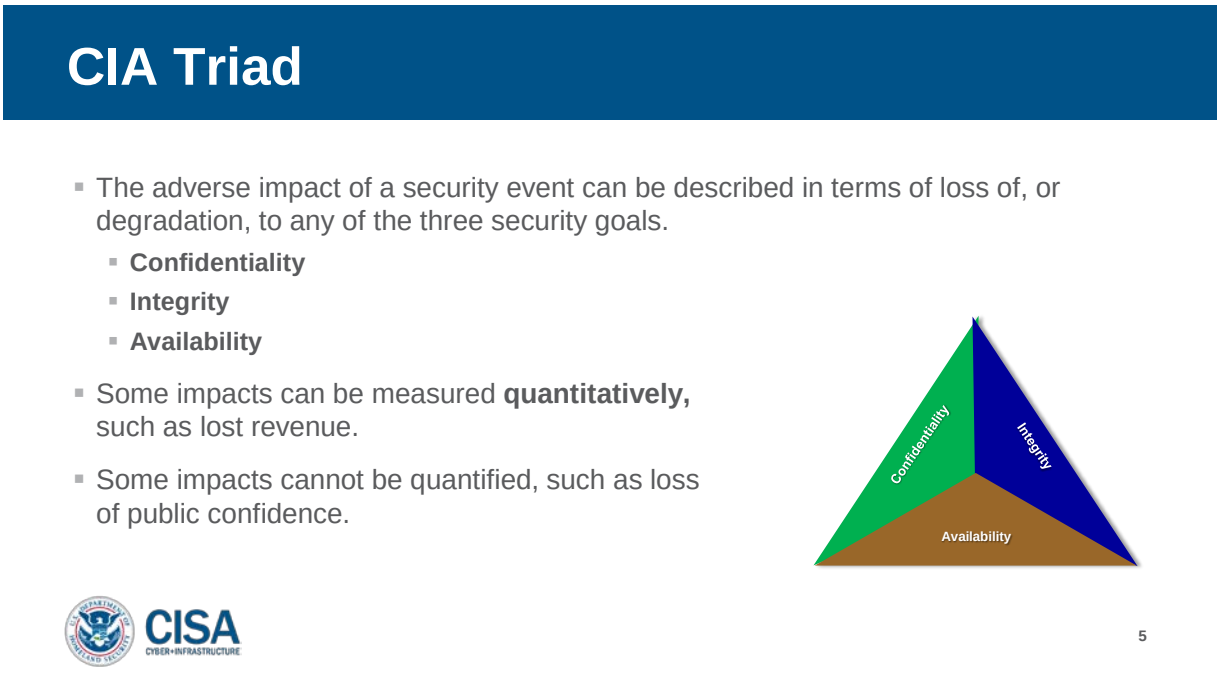
4

**004 So now that we have that down, let's talk a little bit about this assessment. Now, when we're assessing risk. the good news here is there's tons of resources available to you. The key point here is regardless of whatever standard you decide to use, you really need to have a standardized and regular process that could be applicable across the entire organization as best as possible. Sure, you may have certain elements that are specific for, say, a cyber risk, but let's face it, if I'm using OCTAVE, which is a generalize cyber risk assessment, I could actually really easily gear it to other risks in the organization. As long as I'm keeping that as a standard toolset, it may be helpful to maintain that, so now when I'm prioritizing risks, I have an apples-to-apples comparison when the assessment's done. This includes

working at system levels and application levels as well.

Remember, the key is we're trying to identify the threats, the vulnerabilities, and the potential outcomes that could happen to your enterprise, and there are a number of ways that you can get to this as well. You can have certain vulnerability tests of your IT systems; pen testing would tell you how those vulnerabilities would be capable of exploiting-- or, I'm sorry, how the vulnerabilities could be exploited by certain threats; and at the bottom line, you want to find out how you feel pain in the organization. That's related to the outcome.

CIA Triad



**005 Now, another lens to look at this is through the CIA triad. Extremity, for information assets

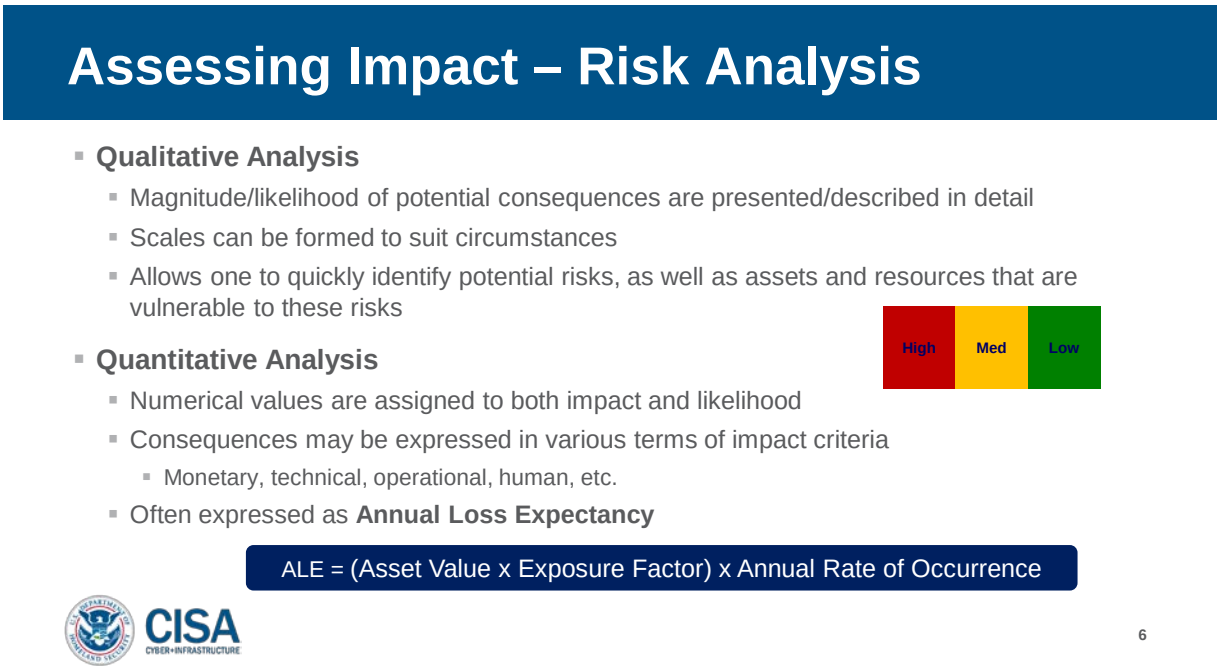
especially-- and of the assets, there's people, there's information, there's technology and facilities. Information is really hard to get your hands around, especially in terms of quantifying the value of those assets. Sometimes it may be very easy, but if you're having a challenge with this, consult the data owners; consult the information owners as well. Those may be two different people, by the way. And you may find out that there's certain elements of that data or that information that you want to remain confidential, to stay within the bounds of the organization. So there may be certain threats that want that information. That's going to change your assessment some. You may be concerned about a threat getting into the organization and changing that information to be malicious, so that way now your information is incorrect that you're gleaning from that data. That would be an integrity issue to think about. Or they may just be interested in shutting your whole organization down and denying you the use of that information. This would be an availability challenge as well.

Regardless of whatever frame or mindset that you're looking at this in, you want to try to get as quantitative as possible in terms of how you're losing revenue.

Let's talk about that availability matter as an example. Suppose I have an organization where if I have a ransomware that shuts down my operating system, then I can no

longer deliver orders to customers. There's clearly a clock running and an amount of money that I could be making within that clock before I get the system back up and running again. This would be an example of how I use the availability frame to understand quantitatively how I'm losing, or feeling impact in the organization.

Assessing Impact – Risk Analysis



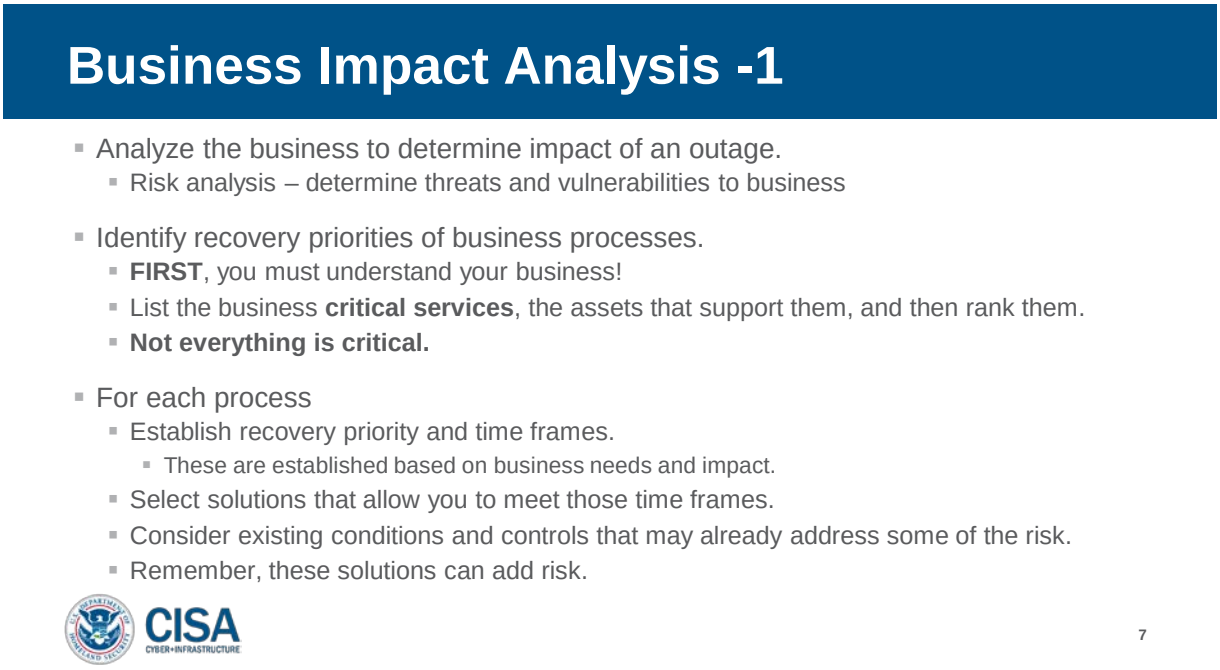
**006 So there are two major types of flavors for assessing risk. One is a qualitative analysis. A qualitative analysis-- think of it as using words to define how your organization is going to be impacted. And by the way, it's not just the impact; it could also be the likelihood. You can use some indices or some scales that can actually define what those impacts are. You could use terms like high, medium,

and low. I recommend that you go look at FISMA and FIPS for these kind of definitions, by the way, if you're thinking about IT security. It would be FIPS 199 and 200, to get additional information on that. Either way, what it's doing is allowing you to quickly characterize what those risks mean to your organization.

But let's say that you have to get to that next level. If you want to get another level of understanding of your risk, you really want to try and get quantitative with it. You want to assign numerical values regarding your impact, or maybe the likelihood of that risk coming to fruition in the organization to really understand what that risk means to you.

Now, you can talk about this one way in terms of an annual loss expectancy. Suppose I know the value of the asset that I'm trying to protect, and I also know that there's a certain degree of vulnerability for that asset. It could be translated into what we call an exposure factor. And we also know, maybe from benchmarking across an industry, or maybe across an organization, or maybe within the federal government, we understand how often that piece of equipment is victimized based on this risk, and that would be kind of like an annual rate of occurrence. If we compile those and we multiply them together, we come up with an annual loss expectancy. All things being equal, this would be a good start.

Business Impact Analysis -1



**007 There are other ways we can go about this too. Let's talk a little bit about business impact analysis.

So what we really want to do here is we want to understand how we feel pain in the organization if these risks are truly coming to fruition, and what we want to do is we want to use what that impact translated to for us to identify what we need to do in terms of reclaiming critical service. So if we lose one asset, is there a way to still provide that service despite losing that particular asset? And what you're going to come up with here is that you're going to have a list of prioritized assets that you need to insulate from this risk coming to fruition.

The trick here is that not everything is absolutely critical. You may find

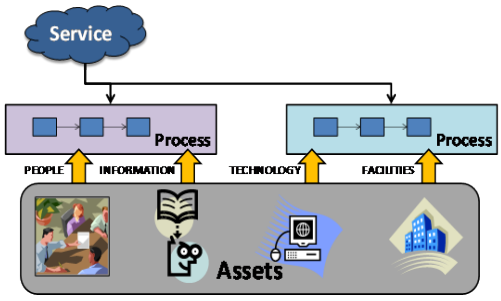
that there are some good-to-haves and nice-to-haves, versus things that are absolutely essential to deliver critical services in your organization. By the way, rely upon your subject matter experts. Rely upon your process experts to tell you what this means, to identify the assets that are truly critical for them to keep operating.

Now, for each of these processes, you really want to understand too not only the importance or the value of the asset that they may lose, but you also want to understand that if they do lose that asset, how long can they afford to have that asset out of commission before you can actually get it reconstituted? So that timeframe will really help you understand how much resource you need to invest in it, if I need to eliminate a risk altogether from happening to it, or maybe if I can afford to have impact from a risk happen, and I really just need to pay into maybe some disaster recovery or some kind of business continuity practice that could really help me in the end too, or maybe both.

So you want to search for the most economic solution in that regard, and that's why we use business impact analysis. Remember too, no matter what, you may have in fact control risk that may be inserted when you actually apply these controls to the risk that you have identified.

Business Impact Analysis -2

- Address four main **asset types.**
  - **People**
  - **Information**
  - **Technology**
  - **Facilities**
- Consider critical dependencies supporting elements critical to operations.
  - Vendors, suppliers, other organizational functions
- Define and assign a criticality rating to each impact.
  - Mission-critical, vital (essential), important, or minor



CISA CYBER+INFRASTRUCTURE

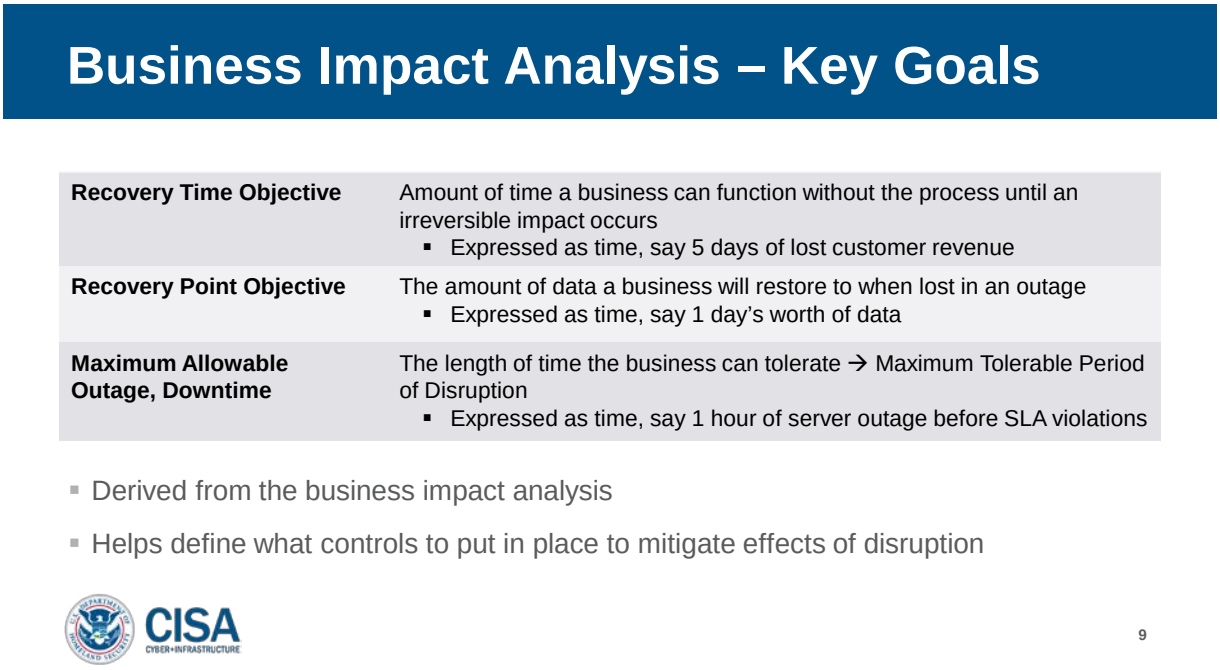
8

**008 So, like I said before, There are different asset types that we need to consider. People-- and by the way, it's not just people in terms of their physical well-being; we're also talking about the information that they may have, maybe critical skills that they bring to the table. You may be talking about information in their systems. By the way, people may be containers for information. We'll get to that in a few minutes.

You may also have this notion of technology. So these are your databases, your mainframes, your systems that are actually storing said data, or it may be not even that; maybe it's communications technology, or maybe it's vehicles or other large capital assets. If you're a navy battle group, maybe it's ships.

You also want to think about it in terms of facilities. What's actually housing these assets? Because damage to one may incur damage to another. For example, if I have a facility that is housing all my databases and it catches on fire, I have a problem. Now, I've looked at that facility in terms of an asset, but now I've also looked at it in terms of it being a container. It's actually storing other assets. So that may be yet another lens that you want to think about if you want to start digging down into the details of how a process can truly come off the rails if a risk were to come to fruition.

Either way, you want to consider how all these assets rely upon each other, and as you're doing that, don't neglect third-party suppliers and vendors who may also be providing similar services, or provide critical services to you, from any number of different assets in these same categories. It's important as you go through this to put some kind of label on it to understand how critical these assets are to your organization. Is it important to you, or is it maybe just a nice-to-have, like we had talked about-- a minor contributor.



**009 So we want to think about this in terms of, like I said before, if you have a risk that comes to fruition, you may have an asset that goes out of commission, but at the same time you can afford a little bit of time to bring it back up online, so that way you don't have to have multiple assets of the same flavor. That may be too expensive. So we want to define how it is we're going to think about these business impacts in terms of maybe a recovery time objective. So this is the amount of time that a business can function without a process going on, and yet having impacts to the organization that could be irreversible, or so damaging that the business can no longer continue.

You may also want to think about this in terms of recovery point

objective. Now this is the amount of data that a business will have to restore when you've had an outage. So suppose you've had someone who's denied availability and access to one of your servers. At some certain point, if you're capturing a data stream, you have to understand how much of that data stream can I lose before I have some irreversible damage to the organization as well. You may also want to think about this in terms of the maximum allowable downtime that you can have, or period of disruption.

Now, some of this can be transferred away. I can buy business interruption insurance, for example. But there's going to be a point where that organization is going to feel so much pain, it may be irrecoverable. So we think about this from our business impact analysis, and it helps us really understand what controls we need to put in place.

Gap Analysis

- This step is often overlooked, but it is actually where a large impact can be made.
  - A big part of risk management is prioritization of resources.
  - Imagine the value provided by eliminating replication of resources that already exist or are being purchased for other risks.
- General flow of events
  1. **Analyze current state**
  2. **Develop strategy for improvement**
  3. **Communicate and manage risk**
- Applies to risk, mitigation strategies, among others

CISA CYBER+INFRASTRUCTURE

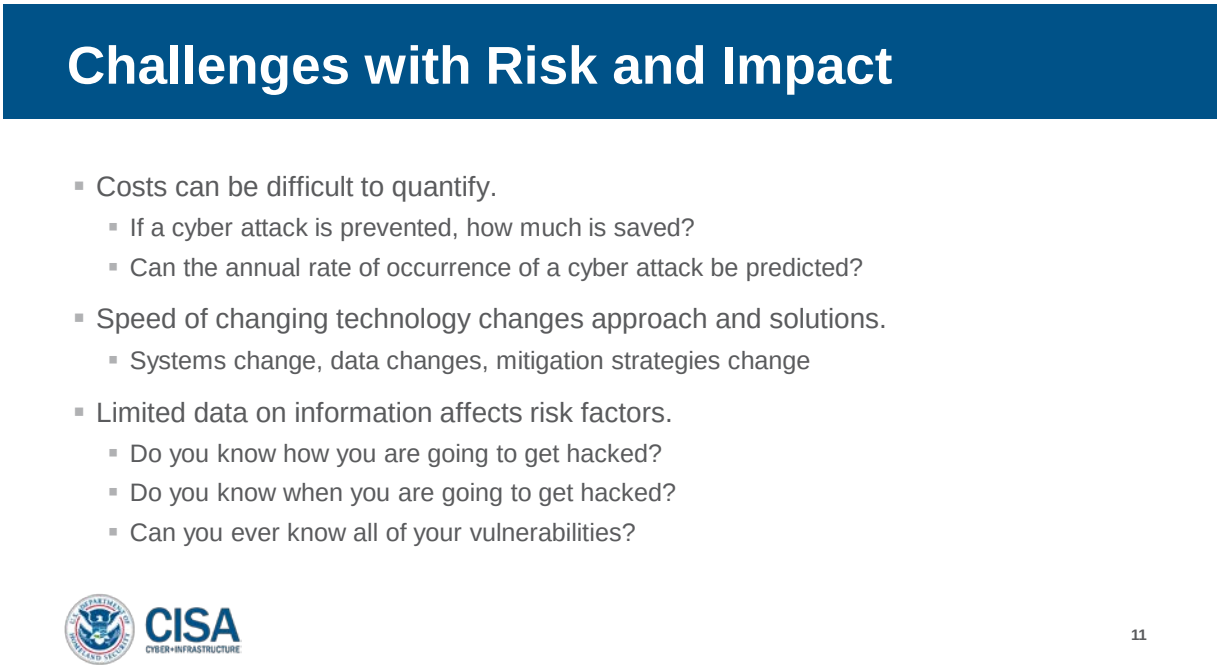
10

**010 We may also think about this qualitatively if we're talking about gap analysis. So, what we really want to do here is we want to understand what the resources are that we're using to control these risks, and we want to talk about how we're going to prioritize them. Now, imagine if we have resources already in place in terms of controls and we've actually replicated them and we're actually just spending money where we shouldn't have to. A good example of this is if I'm preventing fires in a building, and I already have a sprinkler system in place; I have fire extinguishers. I don't need to buy those again. But maybe I'm so concerned, maybe I have to go out and actually hire a fire brigade. That would be yet another amplifying control or a complementary control that we could actually use, and it's a

wise use of resources because you're not replicating resources that you already have in the facility that you're trying to protect.

So if we're going to do this gap analysis, we want to think about not overspending, if you will, to control our risk. We really want to look at the current state of the controls in our organization that we have. To enter into that argument, you really want to consider the risks that you have too, so you're going to have to come to the table with both those and understand the organization in terms of what they're controlling and an understanding of the risk profile that you may have.

And then you want to think about, "Okay, so given this risk portfolio that I have, the profile that I'm seeing, the exposure that I have, what would I do to actually control that situation better?" And then what you want to do is you want to talk to your stakeholders, whether they're you're sponsors, working up in your organization, or whether it's the subject matter experts working down in your organization, to understand what controls they think would be best implemented in that particular case to manage that risk.



**011 Now, a challenge here is that these costs can sometimes be really challenging to quantify. Requirements exploration is really important in this case, especially in terms of cyber. You got to understand that a lot of this information that we may have in systems, it may be good information today, but given new technology and a new day, it may be superlative information that we can't live without tomorrow, and we really may not be able to see that at this given point. So what we need to do is understand and think ahead about what the value of that asset is going to be in a future state just as much as we do today. That can be really hard, and I really don't have a very good answer there, aside from saying you have to really think and work closely with your strategy organization to

understand what an annual rate of occurrence could be if you had a cyberattack that actually took place and took advantage of either the confidentiality, integrity, or availability of that information.

You got to keep in mind that technology is changing a lot. You got to kind of get your mind ahead of that and understand where all this could come together to really harm your business.

So maybe some things to think about in this case is do you know that you're getting hacked or not, and do you know when it's happening, and how often? Can you ever really know all of your vulnerabilities? It's important to kind of get your hands around these and to see subject matter experts not only within your organization but within the industry and otherwise to be able to answer these questions best.

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