Critical Assets and Operations

Table of Contents

Assessing Risk -1

- A Risk Assessment involves the systematic identification and prioritization of risks to information technology resources.

- **Analysis includes**
  - Valuation of assets
  - Identification of threats to those assets
  - Assessment of vulnerabilities in controls protecting these assets against identified threats
  - Calculation of risks
  - Identification of cost-effective controls to mitigate risks

CISA CYBER+INFRASTRUCTURE

2

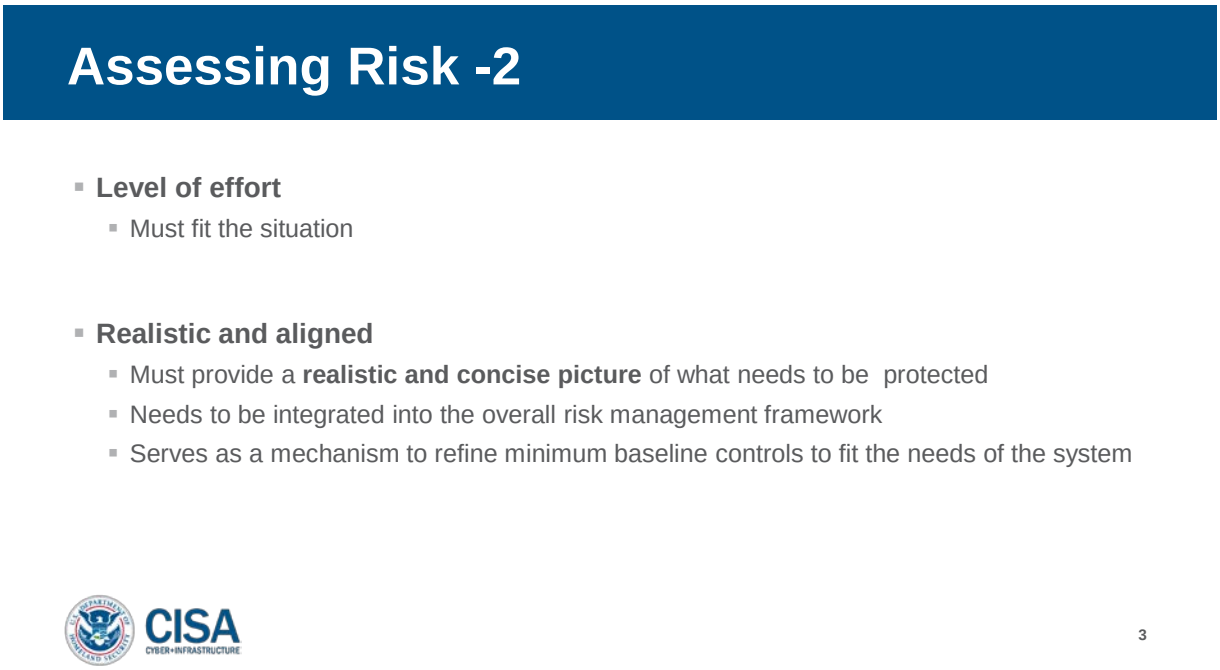
**002 Instructor: We're assessing risk, and remember what we're trying to do is we're trying to identify the greatest uncertainty in any given organization, especially as it relates to information technology resources, and this is going to have a broad range of things that we're going to cover. One is we have to understand what the critical services are in our organization and the assets that deliver those services.

As we do that, we need to understand what is the value of those assets to the organization? We have to also understand what threats are opposed or are trying to take advantage of or exploit those assets as well? And we also understand too that once we know what the threats are, or at least we think we understand them, and once we know what our assets are, our critical ones,

at that, we want to know what we can do to control that situation, what we can do to reduce the uncertainty of the likelihood that we're going to actually have any organization, any threat or threat actor, exploit that, those assets.

This comes down to a process we're going to actually calculate what those risks are. We're going to try and quantify them as much as we qualify them to understand how to prioritize them, and once we have them prioritized, we can identify what resources we want to commit to implementing those controls.

Assessing Risk -2



**003 So let's talk a little bit more about how we assess these risks. One thing you need to understand is that there's--any given amount of effort that goes into this process has

to somewhat be proportional to what you're going to get out of it. So if we have tactical risks, we're not going to spend a whole lot of time at the front lines talking about the safety related to one evolution.

A classic example would be suppose I'm at a construction site and we need to dig a hole, and we may need a box to fill out that hole so that way people don't--are not injured by a cave-in. Well, that's one risk, that's one situation, and it's not going to take long to figure out that the control is to put the box in the hole so that way we can keep the people protected. So in this particular case, and we switch back to an IT perspective, we really want to avoid spending so much resource level and effort on threats that are lower level or maybe even assets that we don't necessarily value as much. Maybe there's higher priority in this. It's not that we don't value them. It's just that we have greater priority things to talk about.

So we have to have, to do this, a very clean, concise picture of what exactly it is we're insulating from these risks, and we also have to look at it in a broader context of what's going on within our risk management framework. We have multiple risks within our portfolio, so what we may have to do is we have to consider them in tandem. Because truly we may have some risks that are interdependent of each other. Interdependent and dependent upon each other as well in a sense that we

may have one response for one risk that may account for a control on yet another risk, and we may get a bigger bang for the buck, if you will. Okay.

Once we do that we can establish a baseline of controls that we can use to protect our assets.

Assessing Risk -3

Assessing Risk -3

- **Relationship**
  - Use the relationship between the system assets, threats, and vulnerabilities to tailor controls
- **Results**
  - Must identify and justify risks that should be mitigated or accepted

CISA CYBER+INFRASTRUCTURE

4

**004 We need to-- let's go back to that idea too of how we need to understand the relationships between these risks, and I can't emphasize enough. You know, I often say, "It's hard to be a risk manager." It really is hard, because on your best days, a risk manager, at best, may be able to say, "Hey, nothing happened today. I've done all my work and I've done all my analysis and business has gone as usual." On your worst days, you know, you miss something, the

worst risk comes to reality and maybe it was a black swan or something like that that you had no control over, and now you're really the butt of the organization and people are going to be upset because you missed something.

So where are you going to make the big win as a risk manager? This relationship piece I think is quite often overlooked in this regard. You can spend some time thinking about the interdependency of risk within your portfolio and you can demonstrate the organization and if I have one control set that covers multiple risks, that there's a big win there, in terms of savings to the organization, in terms of efficiency for the organization, and in terms of just having a overall better resilient organization.

So we also have to think about this and frame it in terms of, "What results am I looking for from this analysis?" and, "Ultimately, what are my risk response decisions?" They must be risk-based. Am I going to determine to accept a risk, or I'm going to mitigate it, avoid it, transfer it.

**005 So let's go back to the very beginning now. Initially, we need to gather information. We need to understand what our critical assets are, and we do that by going to different tiers of the organization, whether it's senior management, whether it's business managers, whether it's even technicians or people who are supporting at the tactical level, and we can talk to them through interviews, you know, surveys. We can talk to them through workshops, research, but there's some commonality with these processes no matter which one you choose to opt for.

For example, before you enter in any given interview with somebody, you got to do your homework. You need to understand the questions that you're going to ask, and you have to

actually even get an understanding, if at all possible, of the kind of answers that you're expecting from them. So that way there's really a meaningful conversation that's taking place. That's where the research part may come in. By the way, you may have research after an interview, because maybe you learned something new. So don't discount that either.

Workshops, that's more active. It's more facilitated. You're going to get together. You're going to talk to folks. It's helpful to have a whiteboard in front of you, and you're going to actually list the critical services, and you can follow those services through an organization via process, and then you dial down yet again and you can find out and identify what the assets are related to each of those processes and executing those critical services.

Let's say I have a larger organization and I'm just trying to get a gross perspective of what the organization may have in store. This is where a survey may come in handy. Once again, you want to spend time doing your homework and making sure you ask questions correctly, wisely, such that you're not wasting people's time but you get the answers that you're looking for, the data that you're looking for.

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?

CISA CYBER+INFRASTRUCTURE

6

**006 Okay. So now, we understand what we're looking for and we need to even identify those assets, and people have come forward and said, "Hey, here it is. These are the things I need." Well, now we have to understand what the value of that asset is, and this can be really a challenge. Think about it. Remember, we classify assets as people, information, technology and facilities.

Now, people. Let's just start there. How do you value a person? It's immensely difficult. Once again, it's not even so much the person at times as much as the information that they may have, or maybe the way they think about it, or maybe the products that they have been able to develop on their own. That's a critical resource, and it's really a hard

thing to try to value that asset. Same thing with data, especially when you have big data sets, where you may have a uncertain information picture of what you're drawing upon. Maybe it will be great in the future to have said data set, but for now, you may not have information coming out of it that shows any value. So how do I assign value to that?

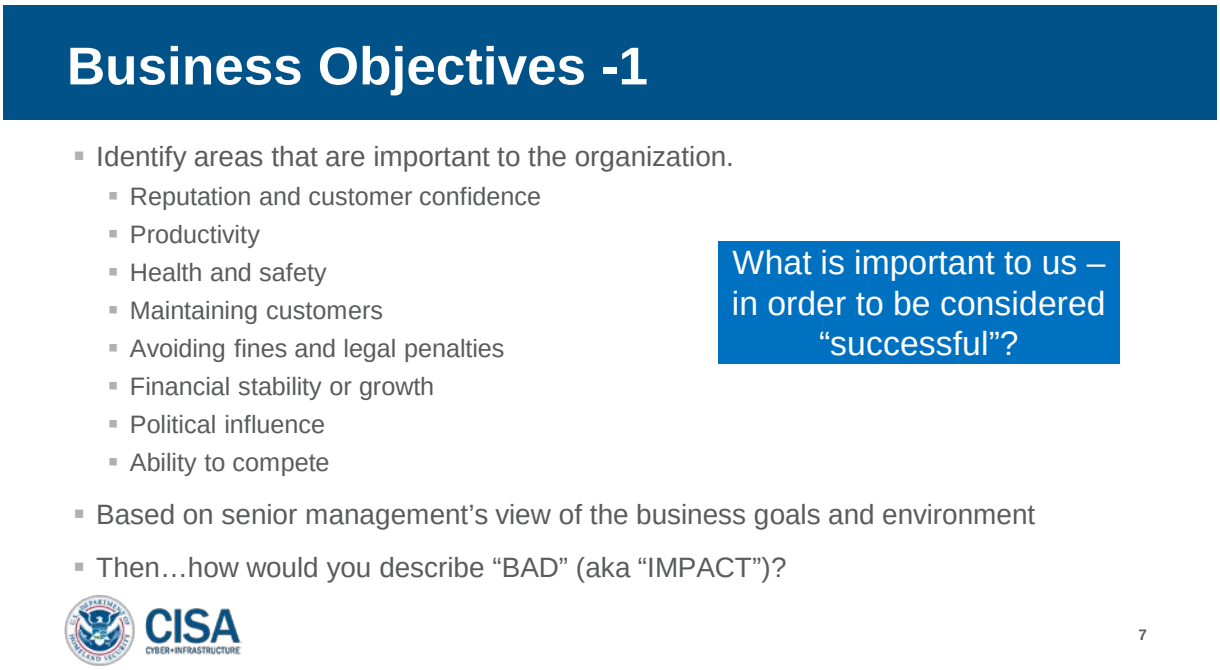
So what I want you to take away from this is don't discount the idea that valuing assets is a challenging process, and you really need to understand how you're going to look at the technical complexity related to it, what control procedures maybe am I putting in place? What not only is the financial loss that I may face, and by the way, it might not be a financial loss. Maybe it's an operational loss. Maybe it's loss of time. So we got to be thinking about this a lot in terms of what we really, truly need in an organization.

And then I may have a qualitative assessment. Based on, like, business knowledge, maybe I have some sacred cows that are the golden calf, if you will, that executive managers really care about and they're directing, "Hey, we need to protect this no matter what." Maybe there's a historical perspective or a culture perspective in the organization that's driving valuation of some assets. Maybe, and this is somewhat the ideal and what you should really look for, is how do you dial those assets back to your overall business

objectives and goals? And there may also be external environmental factors. Suppose you have a regulatory environment that's making you deliver on a certain process. How do you value those assets?

In that game, we call that discussion judgmental valuation. Like I said, ideally, what you really want to do is you want to have these business objectives in line so that way you have a direct line of sight to what you're trying to achieve in an organization and what could really break the process if you lost something that was critical to it.

Business Objectives -1



**007 Let's talk a little bit more about these business objectives, because I really think that this is a key to understanding what these critical assets are, and it comes down

to one simple question. What's most important to us so we can be successful? Successful in managing our business, successful in achieving our objectives. However you want to look at that. However you maintain business. What is it that keeps us being successful at doing that?

So a lot of considerations may come in trying to answer that question. You may think about, "Oh. Well, hey, I have a reputation with my customers and I need to maintain that." May also be this understanding that, "Hey, we need to be productive. If we're not getting product to the market, we're no longer viable." It may also deal with the health and safety of your employees. That actually may be first and foremost on your mind. It may also, and this is especially for an IT organization, you have to maintain your customer base, right. Not only in the sense that they need you, but in a sense, I mean, you're there to support them. You may have maybe some regulatory aspects here. Maybe there're legal fines or penalties that you have to think about.

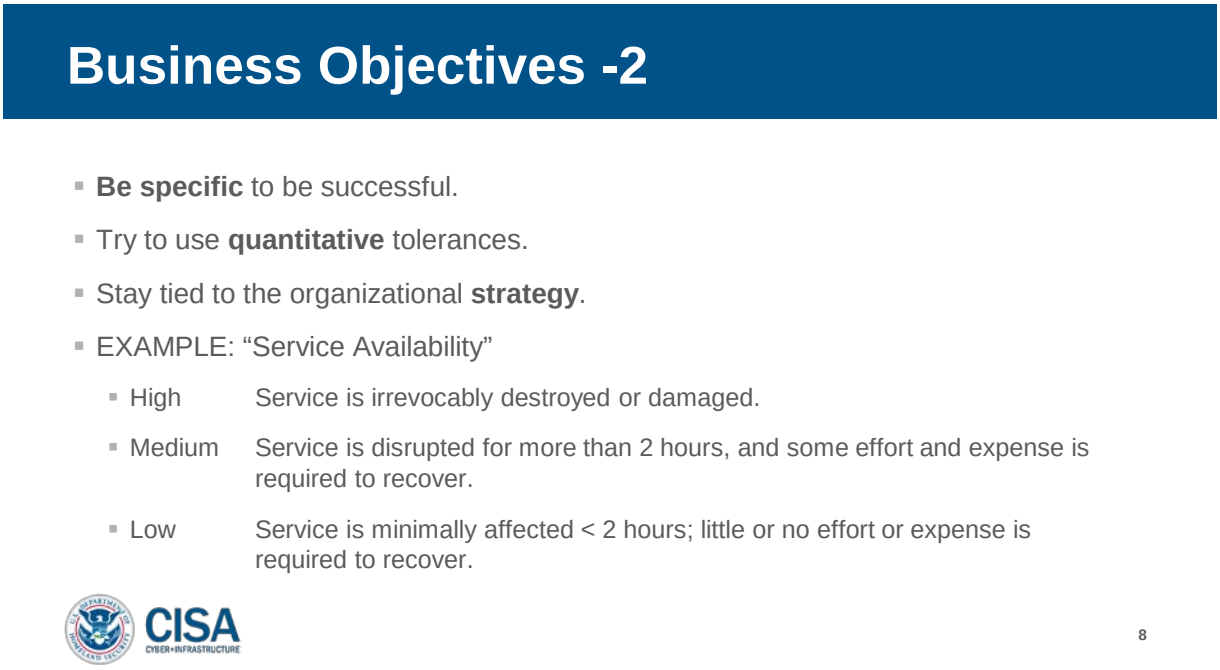
You may have to think about too what is there in terms of competition in the workplace? There may be internal cultural political issues that may be at play, or external. So what we need do here is go back to those processes, those things that we can do to understand these assets better, and I like to rely upon interviews in this particular case. It really helps to

really get and sit down with the subject matter expert or senior management and understand how those business goals tie to the environment that you're in.

You almost want to ask them, one more way to ask this question, is, "What does your coldest, darkest day look like? What keeps you up at night?" Now, by the way, I want to frame that two different ways too. Because sometimes we start thinking about risk as being a negative thing, time, time again. So let me recast that, "What keeps you up at night?"

"Mr. and Mrs. Executive, what keeps you up at night because it's so bad that it would be a detriment to your business?" So that way you're sitting there and you're nervous, you're scared that the organization may crumble, and that's keeping you up. Or counter to that idea, "What is it that there's an opportunity that's out there?" Because remember, that's the other side of the risk coin, and in this particular regard, "What is keeping you up because you're so excited to get in and deliver on this great opportunity? What's keeping you up at night in that light as well?"

I think that if you ask those questions, that one question, rather, in both those different lights, you're going to gear not only a lot of respect from your executive for thinking that way, in a business-minded sense, but also you show and you demonstrate in your analysis that you've thought about all factors to this risk equation.



**008 Now, in all cases too, when you're having these interviews or when you're asking this, questions in a survey, try to be as specific as possible, and this is hard. It's hard work. It's even harder when you try to be quantitative about it. So you have to really sit back and it's not just a matter of writing down questions and going and asking them. You want to think ahead. You want to try to look at the organizational strategy, digest what it's trying to deliver. Think about the measurements of what's trying to be delivered. That's really critical.

An example here could be suppose I'm working on a risk related to the availability of my service and organization, whether it's maybe IT maintenance or maybe it's keeping servers updated or upgraded.

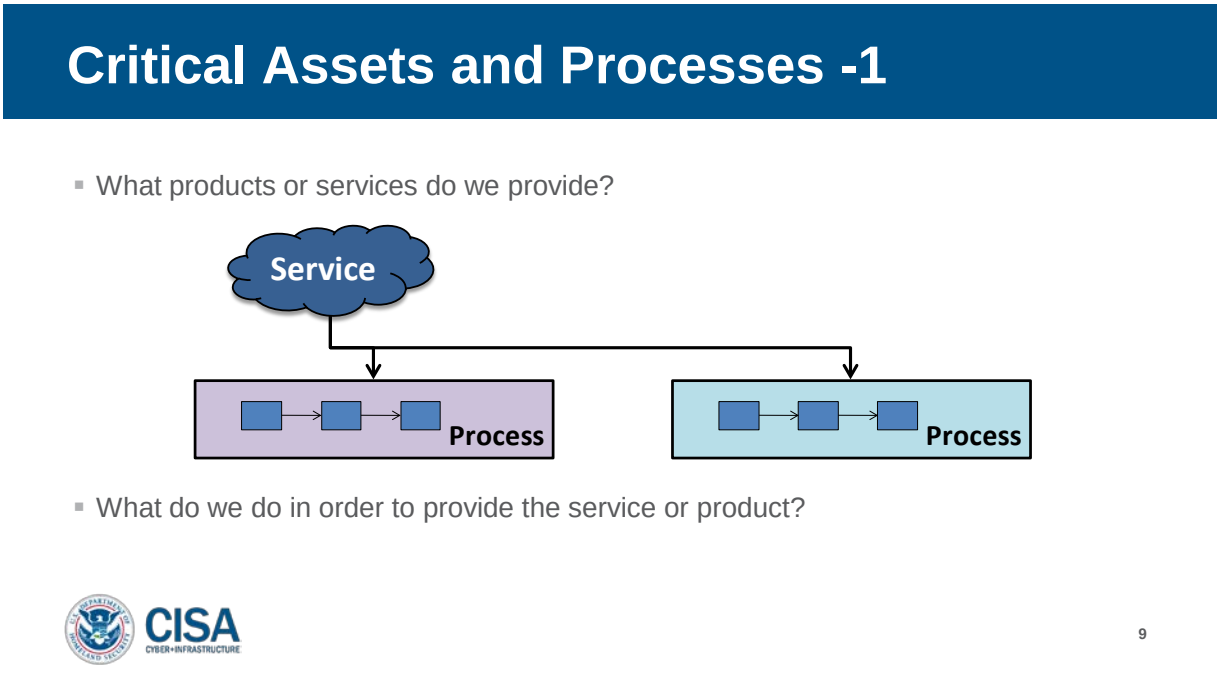
You know, there could be a point where if I'm not doing my work I could have something that attacks the system and the system is destroyed. Maybe ransomware, for example, that just irrecoverably, irrevocably, damages the system that I just can't get it back. That would be a high characterization in my mind, and then from there you can get a little bit more quantitative with this. You know, I understand that it's somewhat binary to say that something is so destroyed that you can't get it back ever, but maybe it's a time factor. Maybe there is a recovery element there.

"So what element of time recovery are you--" Mr. and Mrs. Executive, or subject matter expert, "--what is it that you're comfortable with?" "If it's anything greater than, say, two hours, does that really bother you?" Maybe they shake their head and they say, "No, two hours, I can live with that." "Okay. Fine. Is it four hours?" and keep playing that game until you start pushing their bounds of sensitivity.

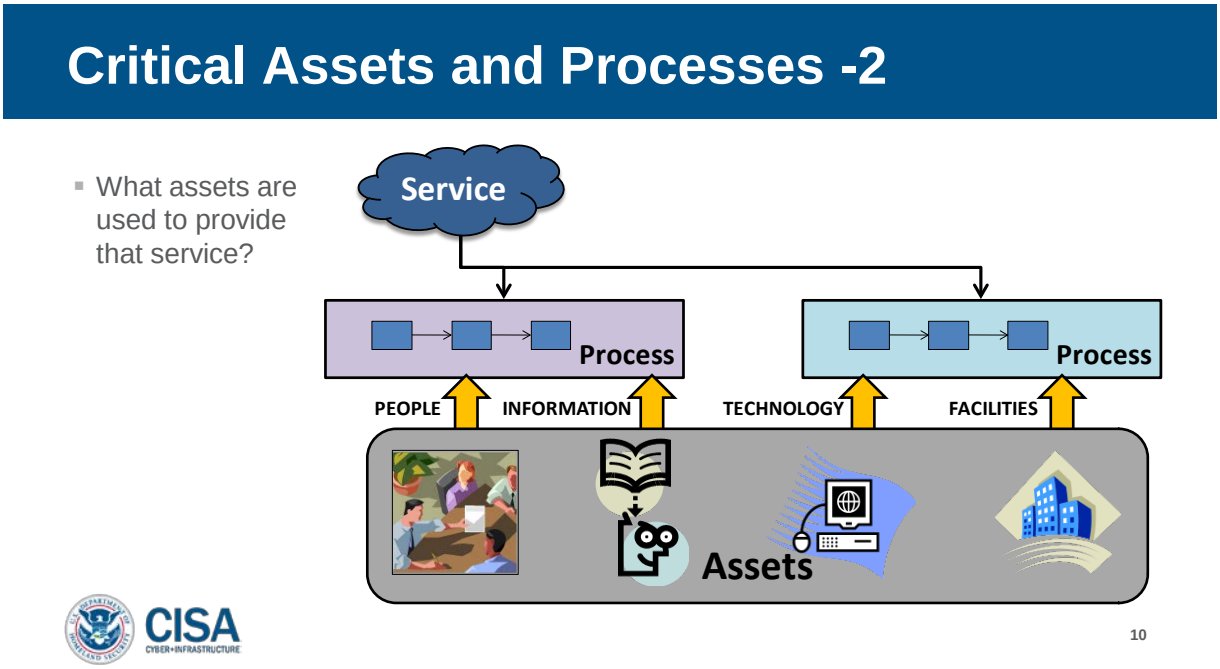
And by the way, this can be a real challenge too, because at times, especially for management teams, executives in a competitive environment, they could be somewhat reluctant to share what their deepest and darkest fears are. So you have to really frame the process and tell them why you're asking these questions before you go and try to just bring it down to base objectives and be in black and white

and say, "Hey, does two hours down bother you?" No. You have to be a little bit more facilitative about this.

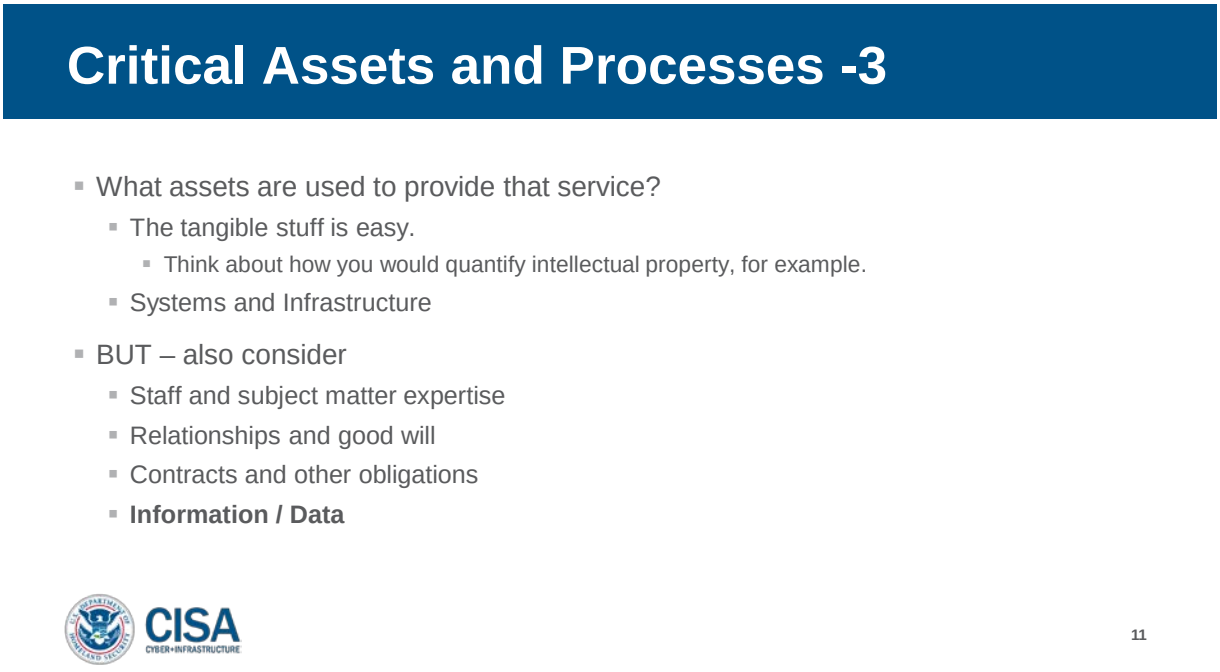
Critical Assets and Processes -1



**009 A way to get to this too is to start out from the basics. "Please tell me what are our critical services? Under your organization, Mr. and Mrs. Executive, what service do you try to deliver? What are the related processes to deliver that service?" And you can see this playing out on a dry erase board even, or chalkboard, where I list what my services are and underneath I can list a string of processes that ultimately deliver that service, and what we can do is we can even go a step further.



**010 And we can start linking what assets are supporting those processes as well. Remember, people, information, technology and facilities are our primary asset categories, and I don't want you to forget too that third-party entities, such as providers, are also a part of that picture.



**011 What we're really trying to do is identify, remember, those critical services, and using that model of people, information, technology, facilities, you're going to see as you facilitate that process, that the tangible stuff, the things I can actually lay my hands on, that actually comes to the surface really quick, and it's a good thing, in a sense, because people should know their assets in that regard. Where it really gets challenging is when you really have to tease out the data sets. Where you really have to figure out, "How do you evaluate and know about intellectual property?"

Remember, that intellectual property may be in somebody's head. It may be in a database somewhere that maybe the person you're interviewing doesn't own. So you have to think

about asking those critical questions that gets to the base of where this information, these assets, exist, and you have to think about and know what the systems and infrastructure are in your organization. Ah-ha. More homework that must be done.

But you also want to think about, "Hey, who in my department, who in my organization, has significant subject matter expertise?" You may also want to think about, "Hey, what relationships do I have within the organization and what relationships do I have outside the organization that I value greatly?" Ah, that speaks to reputation. So that's another interesting facet. Well, think about contracts too. These may be contracts that my organization has where I have to deliver for certain customer set, or vice versa, and this is especially true in IT organizations where I have vendors who are to help me--let's think about disaster recovery, for example. Maybe they're providing a facility that I need to have available, a hot site, if you will. Well, what's that contract like? What are the obligations in it? What do they actually owe me? Those too can be construed as assets with great value, because in the end, if that cold, dark day comes and your organization comes to a halt and you need that hot site, if it doesn't have a certain service, if it doesn't have a certain asset that you need that's on sight immediately, because it wasn't in the contract, you're sunk. So we have to think about that in greater detail.

And I've already talked about the information data piece. Always a challenge to figure out, first of all, "What data do I have? What information am I gleaning from it, and how do I evaluate it?" Furthermore, it gets even more challenging when I have a data set that I have to figure out, "What does the future of that data hold in terms of information I may be able to glean in the future?"

Scenario A Department of Defense Example

Scenario

A Department of Defense Example

- Naval Battlegroup Deployment:
  - Asset identification relates to the critical services needed by the mission
  - Suppose one of the services is to conduct maritime interdiction.
    - What assets will be necessary?
    - Parent ship and supporting command
    - Trained personnel
    - Rigid haul inflatable boats or zodiacs and support equipment
    - Firearms
    - Threat and regional intelligence
    - Communications equipment

  - Now your turn – What cyber assets may be related to this mission?

CISA CYBER+INFRASTRUCTURE

12

**012 We have a Navy battlegroup, and we're going out to sea. We have a carrier, we have cruisers, we have destroyers, we have maybe some subs. We have some air assets. All of that is part of this Navy battlegroup, and what I need to do, as I'm identifying risks related to it, I need to identify the critical assets for that group, and I

can think about this, once again, in terms of tiers, right? I have vessels. Large ones. It's pretty obvious to see that your capital asset is going to be your carrier, especially if it's a carrier battlegroup. But you got to start decomposing that and thinking about more of what's necessary to power that asset as well. It's not just that parent ship. It's the personnel who run it. It's the small boats related to it. What missions do they deliver? It's the support equipment. It's the firearms. It's the ordinance that you have, right? It may be information. Maybe it's a--maybe it's to be thought about in terms of your threats in the region that you're going to and intelligence, and intelligence collection assets. Assets that you may not, in fact, control. It may also be like communications equipment, and that's the technology piece that you're speaking to there.

So I challenge you, if you want, pause. Stop the video right now and challenge yourself to brainstorm some of these assets that may be related to this critical Naval battlegroup deployment. It's truly going to be an important mission. There are things that you have to accomplish. Think through, at least in terms of categories, what you may have to consider.

Data Classification -1

- The practice of **evaluating the risk level** of the organization's information to ensure the information receives the appropriate level of protection
  - Assign sensitivity, criticality, and security priorities.
- Ensures **confidentiality** of information by restricting who can access or copy the information
- Increases accuracy and **integrity** of information by controlling who can modify or update it
- Increases **availability** of information by restricting the ability to overwrite or erase important or critical data

CISA CYBER+INFRASTRUCTURE

Ref: Official (ISC)² Guide to the CISSP CBK

13

**013 Okay. So now I understand that I need to learn about the data that's in the organization. I need to really make sure that this data has the appropriate level of protection that it needs, and we had talked about already the fact that that data could be critical to the operation the organization, but it also could have sensitivity. So imagine if that data were released to the public. Is there anything in there that's sensitive that I would not want threat actors to get ahold of?

That speaks to the confidentiality piece, correct? We need to ensure confidentiality of that information by restricting who can have access to it. We need to think about how that, the accuracy of that data, is important to us, and this comes in with the integrity piece, right? If anyone were

to get into the system and they were to actually change any of the data, that it would actually maybe corrupt the information that I get from the data, then we need to be sure to provide it the correct degree of security as well.

And finally, we want to think about how the data is available. Now, we've heard of ransomware. This is a classic case where we lose the availability of that data to do what we want with it. We can't use it because it's locked down. Or maybe it's erased altogether and we can't access it anymore. This speaks to the availability piece.

Data Classification -2

Data Classification -2

- Avoids **damage** to the organization's **reputation** by reducing the risk of unauthorized disclosures
- Reduces the cost of **overprotection**
- Provides managers the ability to enforce **accountability**
- Protects **intellectual property** and **trade secrets**
- Protects consumer **confidential information**
- Complies with **industry regulation** or **legal requirements** to protect personally identifiable information

CISA CYBER+INFRASTRUCTURE

Ref: Official (ISC)² Guide to the CISSP CBK

14

**014 And once we understand those, we can start setting up our strategy for how we're going to avoid damage to that information. How we

avoid losing it. If you think about it, this could lead all the way back to how other organizations see us from a reputational sense. So there's a lot of gravity and import that we should be putting on how we classify this data.

Now, I also want to go back and revisit the idea that we don't want to build a very expensive, let's say, million-dollar fence, around a stack of pennies. So we really need to be concerned about overprotection as well. With that always in mind, we know that we want to have somebody who is at the fence, if you will, that's accountable for it. We also want to make sure that if we have any trade secrets or intellectual property, that that comes to the top in terms of being priority.

Furthermore, we know too that we have some customer data that we may hold. This is classic in terms of customer credit information would be a good example. We don't want to release that to the public. That's confidential information, and we don't want to expose ourselves to the litigation that comes with actually losing that information. So we're going to have to think about how we're going to insulate that from an attack as well.

We also have to abide by maybe certain industry regulation. A classic example here would be with respect to healthcare information and HIPAA. We need to make sure that that information is protected as well, because we're legally bound to do so.

Classification Program

- **Questions** that must be answered in implementing a classification program include:
  - The number of classification levels required?
  - How to locate information?
  - How to identify classified information?
  - How to mark, handle, transport, store, archive, retain, and dispose classified information?
  - Who is the information owner?
  - Who has authority for deciding access?

CISA CYBER+INFRASTRUCTURE

15

**015 So we have to establish a program so that we can control this better, and we have to ask a lot of critical questions in this process, and it will help guide us down the path. So I leave a few for you here.

For example, how many classification levels do you need? Simple enough. Maybe it's just a black and white two levels. One level is I keep it all in house. Another level is I can share it with anyone I want. Well, we all know that that's an ideal world and that's probably not likely. You're going to have to probably have a number of levels in there, let's say maybe two to three. We'll leave that for a moment and it's going to be discussed in the next slide.

How do you locate the information? Where can it be found? If you think

about it, the location of the information is going to dial directly back to how I'm going to actually provide security controls. Secondly, if the information is readily available to the enterprise, how is it that my staff, my people, or even people external the organization can see it and recognize immediately that that information has a certain pedigree to it, that it has a classification? Do my employees know how to actually mark the information in the proper manner? Do I have a rubric, if you will, to put that data through and have them understand what label to put on that? And furthermore, do they know how to handle it, do they know how to take it from location to location? Do they know if they're even allowed to? Do they know if they're allowed to retain it? Do they know how to properly dispose it?

Now, you can really see this in any organization. I'm sure some of your organization have burn boxes or burn bags, and you can imagine as you walk around the place if you can actually put your hand in that bag or put your hand in that burn box and pull data or information out. Maybe it's sheets of paper or whatever the case may be that's in there, storage media. You know that that is not necessarily a good way to store disposed information.

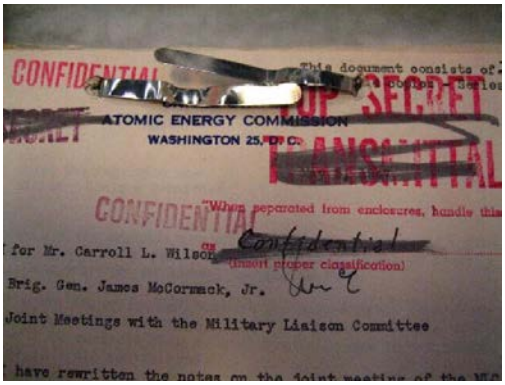
So you have to have, as a part of this program, consideration for how it gets disposed, how often do those bins actually get emptied? Where are they located?

This may also come back to understanding and knowing who the information owner is. We have to know who is actually using the information and dial it back to, "Okay. So if that person is using it, who actually owns it? Who's responsible for it?" And by the way, those two people may not be the same.

Finally, you have to think about who in the organization should get access to this? Largely we talk about this in the information community as a need to know. So if I have information that's confidential, not all people in the enterprise necessarily need it, even though they may share the same security clearance. They may dial back to this notion of somebody has to have a need to know to actually access the information.

Data Classification Criteria

- Public Documents
- Internal Use Only
- Proprietary
- Highly Confidential
- Top Secret



CISA CYBER+INFRASTRUCTURE

16

**016 So as I mentioned before, there are different ways we can classify this documentation, and by the way, if you're an enterprise, maybe two classification levels is adequate. But if you look at some ISO standards, and there are other standards out there that can help you with this, that you can understand that some of these documents may have additional degrees of classification related.

For example, if I have documents that are broadly acceptable to be shared with the public, marketing materials, for example, is a classic example there, I could make those public documents. Suppose I have some documents that, ah, they're not as public as I'd like them to be. Maybe there is some, some information on there, that I would

prefer not to be released to the public. I'd just like to keep it within the walls of my organization. That could be an internal use only.

Now, suppose I have trade secrets or data or any information like that, or maybe even customer data. I may need to ramp these classification levels up to a proprietary level, or even something that's highly confidential or maybe even to the utmost levels of the organization where it's a top-secret kind of an issue.

In those cases, that information clearly is going to have a higher priority in terms of the security that you're going to put around it, and you're going to have actually custodians who are going to have to be more concerned with how they give access to it and what it means to be granted that access. What are those people specifically doing with the information? Those are all things that you're going to think about when you're classifying your documents.

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