Disaster Recovery Plans and Procedures

Table of Contents

Disaster Recovery Plans and Procedures

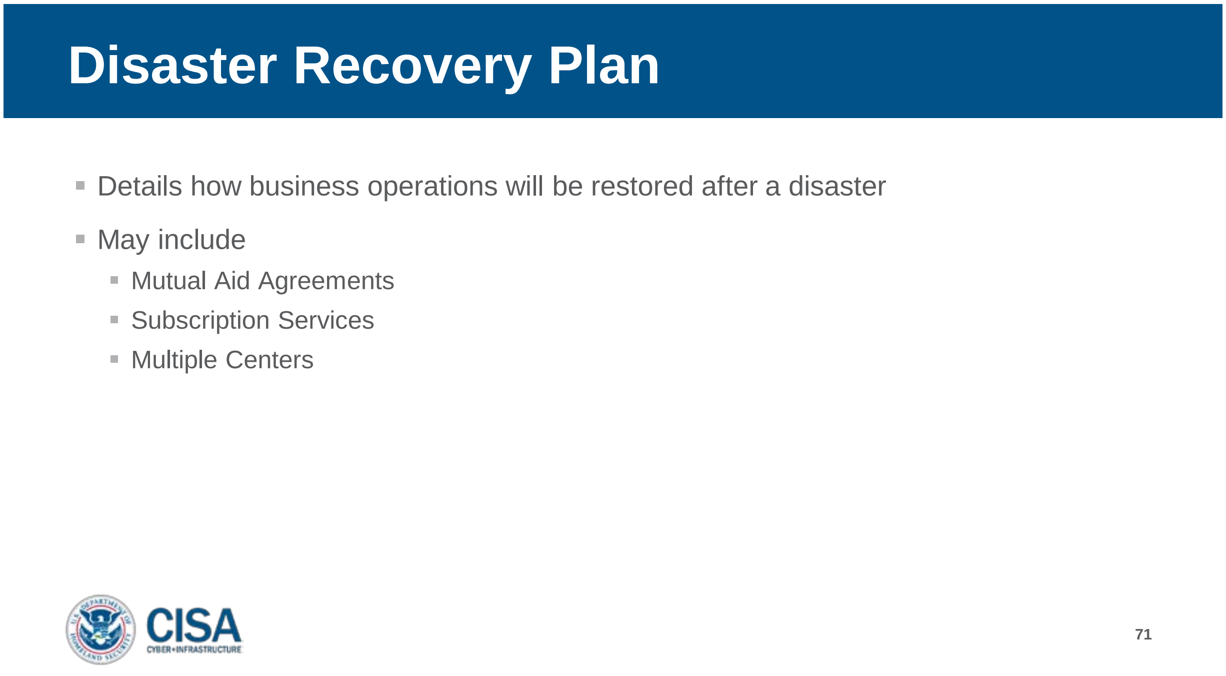
CISA

CYBER+INFRASTRUCTURE

Disaster Recovery Plans and Procedures

70

**070 Instructor: For this particular presentation, we want to talk about disaster recovery plans and associated procedures.



Disaster Recovery Plan

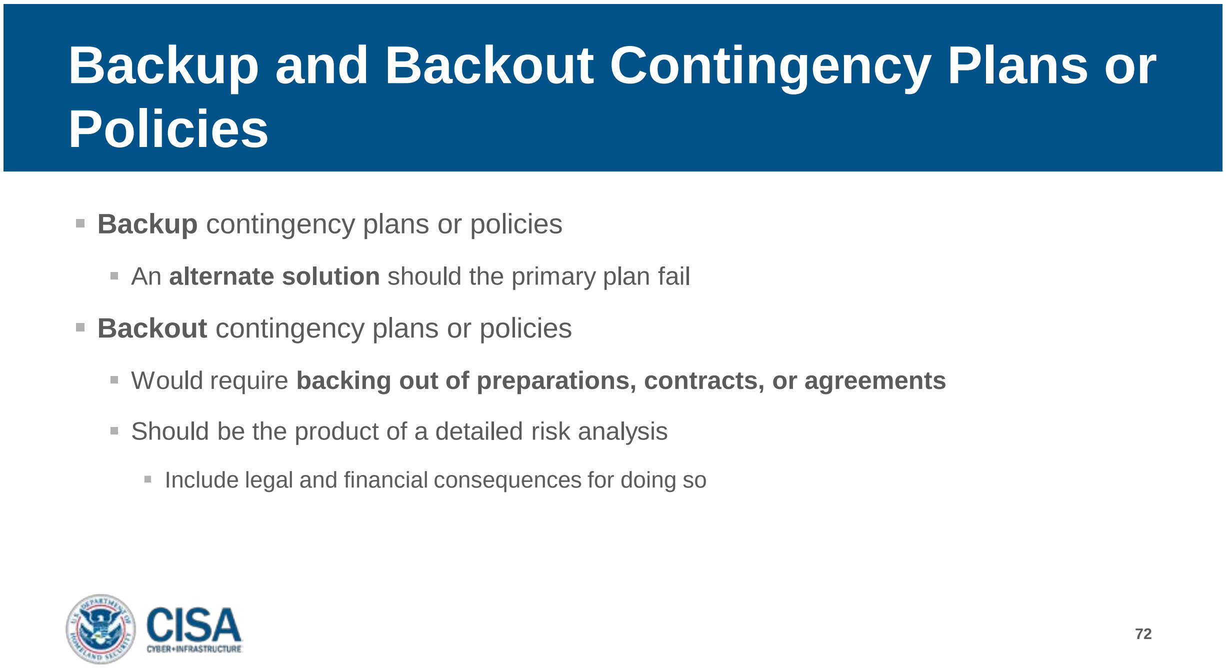
- Details how business operations will be restored after a disaster
- May include
  - Mutual Aid Agreements
  - Subscription Services
  - Multiple Centers

CISA
CYBER+INFRASTRUCTURE

71

**071 So, what exactly is a disaster recovery plan? Well it's just as it says. It's a plan that provides specific detail on what you're going to do when you've reached that darkest day when that risk is realized. There are several elements to this plan that need to be considered, but to be honest with you, it comes down to the organization that you have, the business that you're running, and the goals that you're trying to achieve.

Backup and Backout Contingency Plans or Policies



Backup and Backout Contingency Plans or Policies

- **Backup** contingency plans or policies
  - An **alternate solution** should the primary plan fail
- **Backout** contingency plans or policies
  - Would require **backing out of preparations, contracts, or agreements**
  - Should be the product of a detailed risk analysis
    - Include legal and financial consequences for doing so

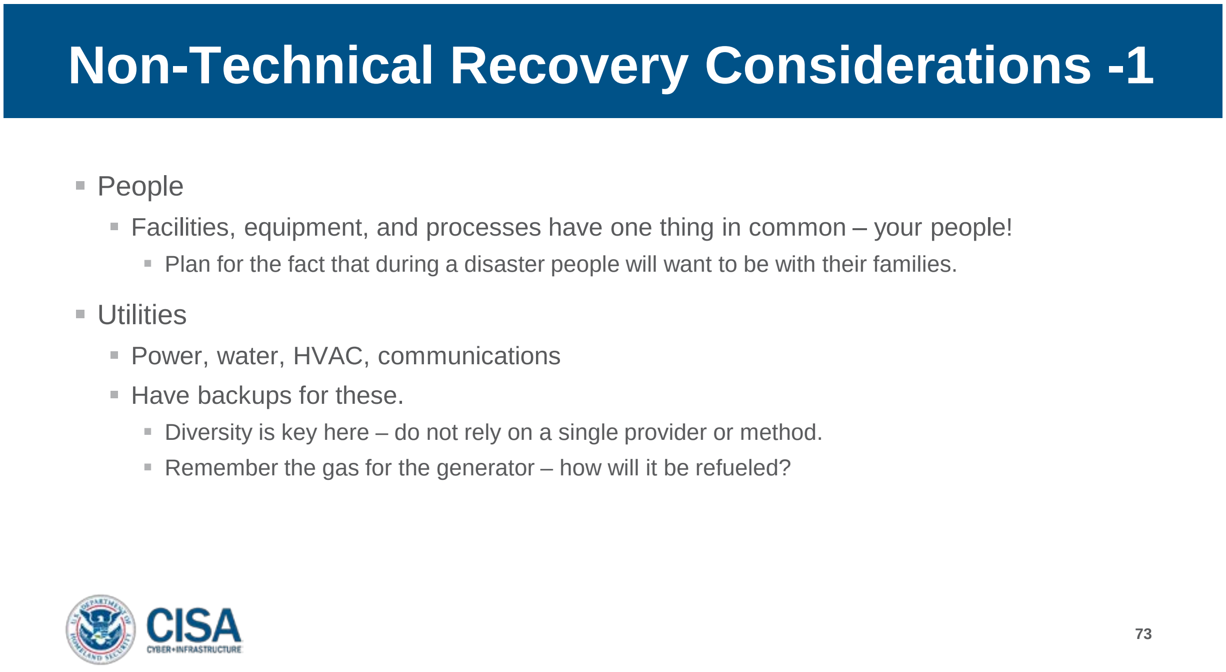
CISA
CYBER+INFRASTRUCTURE

72

**072 You may also have a backup or back out contingency plans. A backup plan really is a plan or a policy that talks about alternate solutions should your primary solutions fail. So, you have a disaster recovery plan, for example, and nothing goes right. You may have to have backup plans in place. That backup plan, by the way, may also already be a part of your disaster recovery plan as alternatives within the plan, so that way they don't have to go actually literally, physically breakout another policy.

You could also have a back out plan. Now, this is talking about how you're going to actually back out of existing preparations, contracts, for example, or frameworks that you have established, so that way you can change paths altogether. This is going to be a very critical business decision. So, actually a good part of that plan is going to discuss how it actually gets enacted, let alone how it's actually going to be executed. In all cases, if you are backing out of these contracts or these agreements, whatever you may have, you're going to want to use legal professionals for their advice so that you understand the full extent of what you're doing in that business decision.

Non-Technical Recovery Considerations -1



Non-Technical Recovery Considerations -1

- People
  - Facilities, equipment, and processes have one thing in common – your people!
    - Plan for the fact that during a disaster people will want to be with their families.
- Utilities
  - Power, water, HVAC, communications
  - Have backups for these.
    - Diversity is key here – do not rely on a single provider or method.
    - Remember the gas for the generator – how will it be refueled?

73

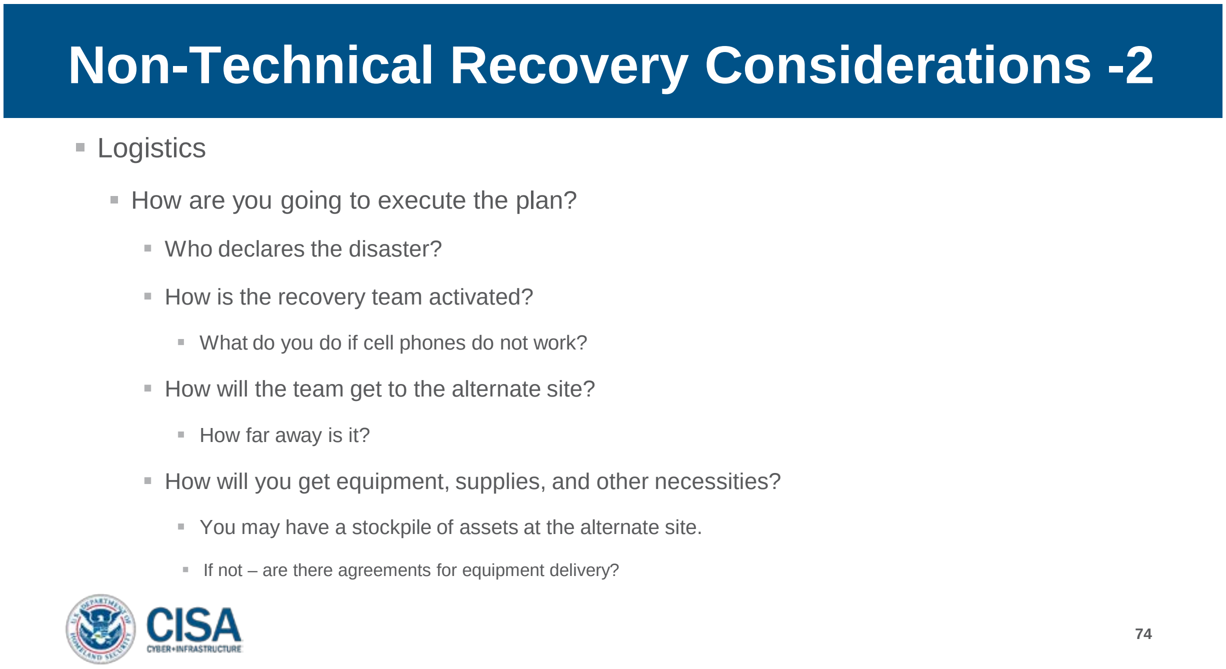
**073 Not everything is technical. What I want you to consider here are elements like your people. In any given event, especially the big force majeure ones, think about a whole area that's taken out by a hurricane, for example, or maybe tornadoes, your people are critical to getting your operations running, but they live lives outside of your organization.

You've got to think about them, their families, and the things that they care about first.

Now, there are a whole lot of neat tips and tools that you could use here. A good example is, as a practice, is if you have a major event that goes down like this, you could have preloaded credit cards that you issue to each of your employees, right on the spot. Tell them to go home. Tell them to use that money to pay for food, diapers, any essentials that are necessary for their family to get up and stay up and running, so that way they can get back to you as quickly as possible and help get your organization back on its feet.

You also want to think about things like utilities. Do you have power? Do you have water? Do you have HVAC? Do you have phonelines? And that means hard ones too, not just cell phones. And you're going to have to think these things through if you have backups, backup diesel generators, for example, for power. Diversity is key here. You have to think through different scenarios and understand when you may need that backup and how it's going to be implemented.

Non-Technical Recovery Considerations -2



Non-Technical Recovery Considerations -2

- Logistics
  - How are you going to execute the plan?
    - Who declares the disaster?
    - How is the recovery team activated?
      - What do you do if cell phones do not work?
    - How will the team get to the alternate site?
      - How far away is it?
    - How will you get equipment, supplies, and other necessities?
      - You may have a stockpile of assets at the alternate site.
      - If not – are there agreements for equipment delivery?

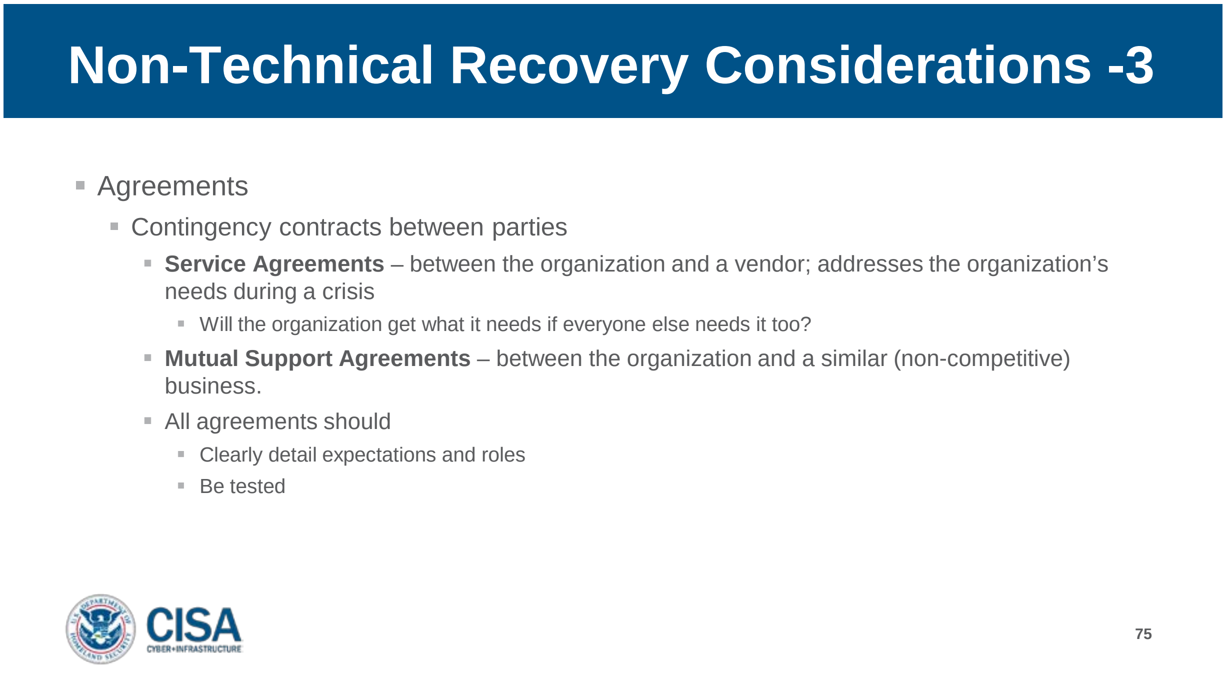
74

**074 You have to think too through the logistics of the situation. How are you going to actually physically execute the plan? How are people going to get to where they need to be? We've talked a little bit before, but I want to reemphasize here the idea that there's going to be this notion about business decision being made as to whether or not a disaster is actually even occurring. You have to define what those tripwires are, and you have to understand who is making this call. Who is actually going to say that an incident has taken place and that you actually have to take actions related to that incident response plan?

This may cost money. It may cost a ton and it may mean a significant interference of your operations--interruption of your operations. You want to think about how that team gets activated and what are they going to do. And what do you do if you lose your primary means of communication with them? You're also going to want to know how you're going to get that team to an alternate site to get things up and running, especially if, once again, you have one of these large force majeure incidents like that hurricane in mind that prevents them from getting to that site altogether.

You also want to understand how you're going to get the equipment, the supplies, and other essentials that are needed to run your operation to that said site. Now, clearly, you may have a stockpile of assets that are already waiting at that site. But if it's a cold site, and it's just an empty space that you're going to be using, you're going to have to figure out the logistics behind getting the new equipment into that space such that you can get things up and running.

Non-Technical Recovery Considerations -3



Non-Technical Recovery Considerations -3

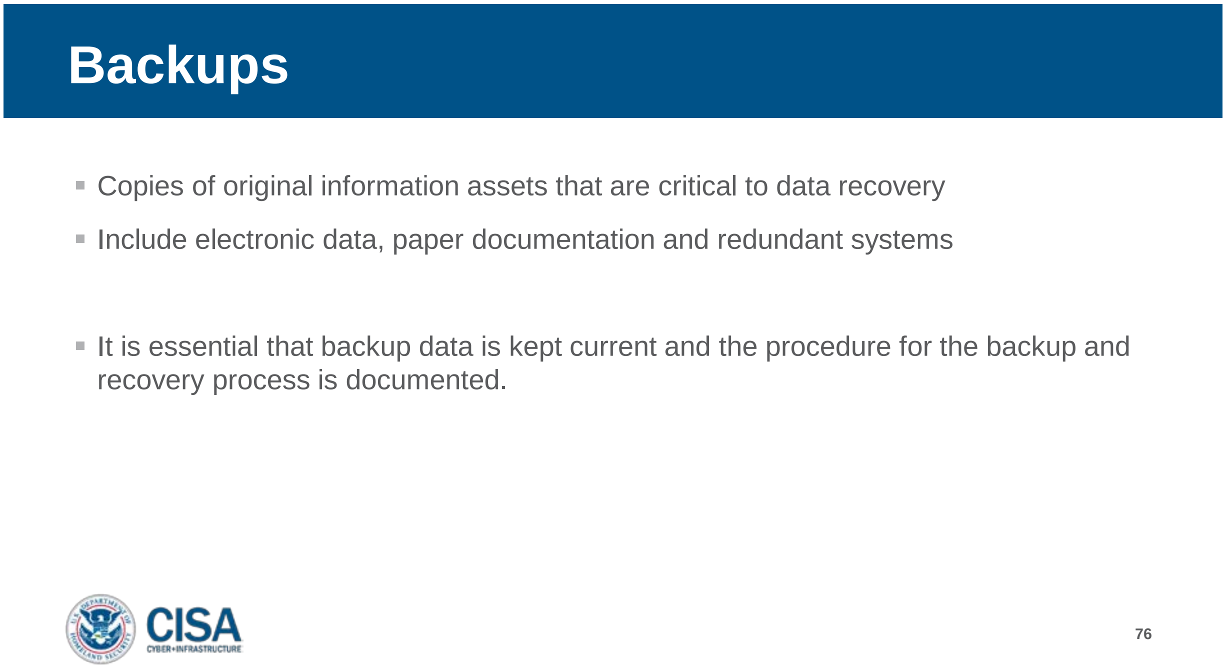
- Agreements
  - Contingency contracts between parties
    - **Service Agreements** – between the organization and a vendor; addresses the organization’s needs during a crisis
      - Will the organization get what it needs if everyone else needs it too?
    - **Mutual Support Agreements** – between the organization and a similar (non-competitive) business.
    - All agreements should
      - Clearly detail expectations and roles
      - Be tested

**075 You're also going to want to take into consideration what agreements you have in place. Think about your service level agreements that you may have with other organizations. For example, suppose you have a cold site across town, and you know that you're going to need it if, in fact, your facility is out of commission. You go to use that site, and you come to find out that the person who has made the agreement with you has done the same agreement with two other companies in the area, and they're also affected by this large incident, hurricane, tornado, whatever it may be. There's going to be a bind. You're going to be trying to fit three different customers in the same site. That's going to be troublesome. You want to make sure that it's exclusive, in that case, to you. This is what I mean when you want to review your service level agreements and make sure that they actually have in it the services that you need and demand.

You can also add mutual support agreements, and this is when you go from one organization to the other. Now, typically, these organizations are similar to you, and largely they should be non-competitive. Remember, if they're mutual, you may end up in the same space. So, you want to think about how you're going to insulate your intellectual property, trade secrets, things like that, so that way there's no bleed over when you're in the same space and you're operating in the same area. There needs to be a clear understanding of what those expectations are, so that way there's no question when the day comes.

And once again, make sure you test it. Get in the same space with those folks. Make sure that they know what they need to do and what you need to do and how you're going to maintain these boundaries.

Backups



Backups

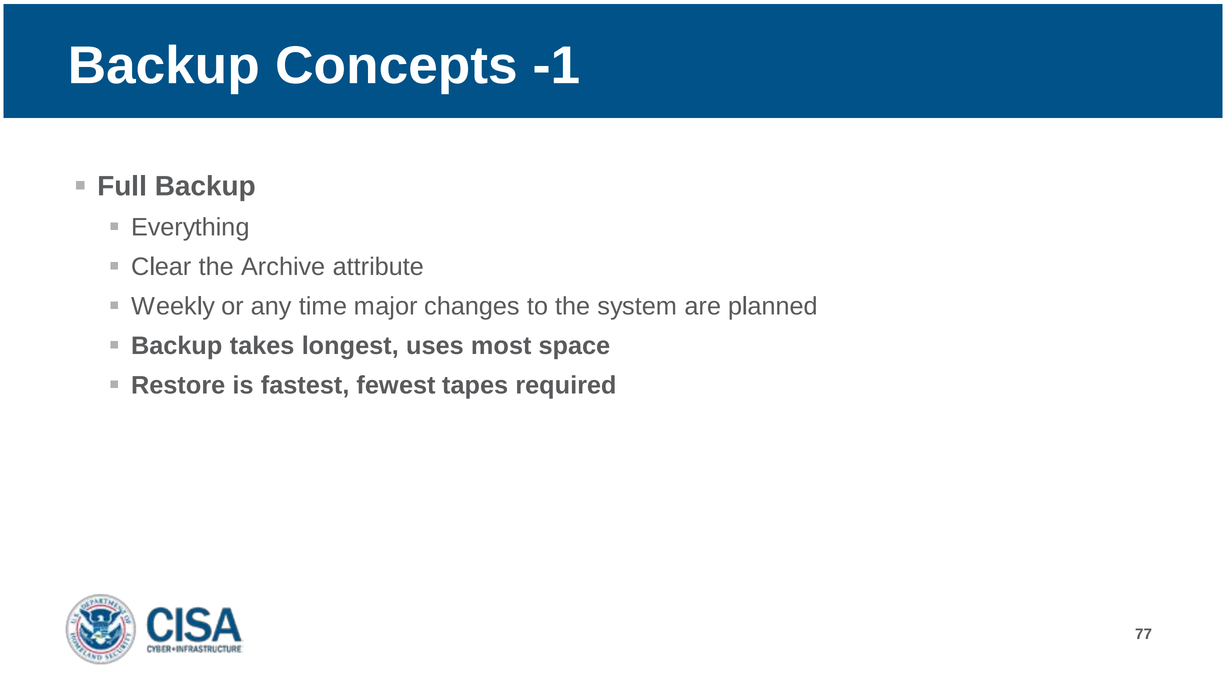
- Copies of original information assets that are critical to data recovery
- Include electronic data, paper documentation and redundant systems
- It is essential that backup data is kept current and the procedure for the backup and recovery process is documented.

CISA CYBER+INFRASTRUCTURE

76

**076 You're going to have lots of data. And it's going to be hard to recover it, so you've got to think about backups. This can be done in any number of ways. And it's not just the electronic data, too. Maybe you have a stack or a file cabinet of papers that need to come with, critical policies that you need to have immediately on hand even before you get that computer turned on. Make sure that whatever this backup is that it is the most relevant and most recent of backups that you've made.

Backup Concepts -1



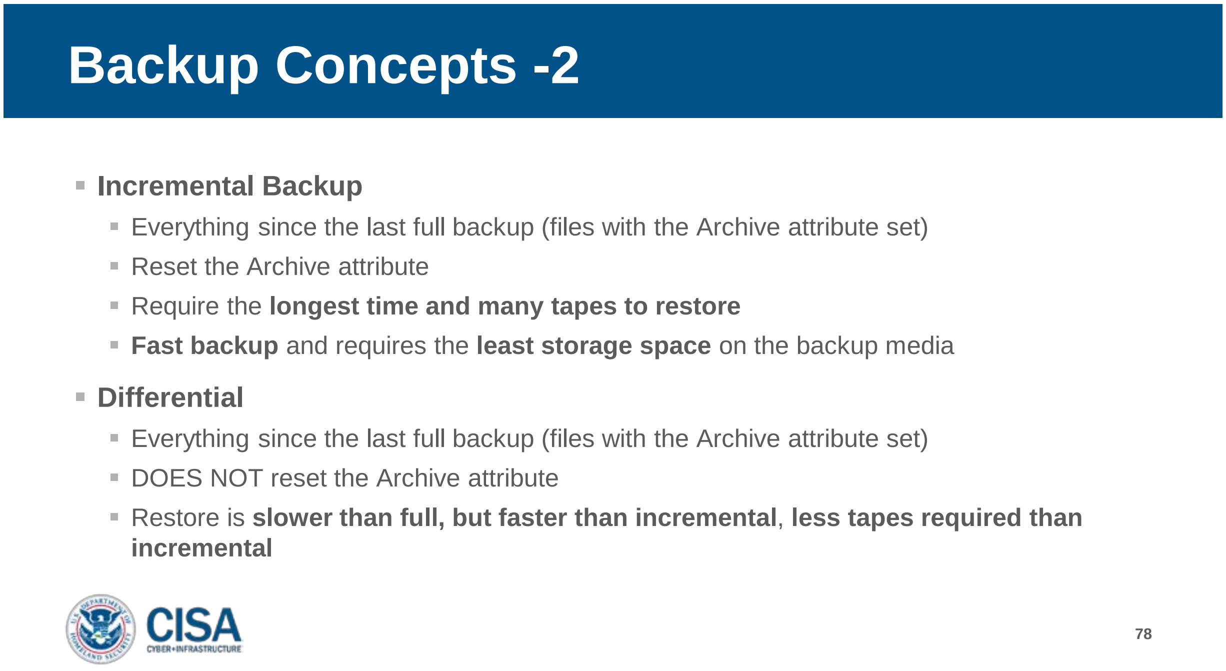
Backup Concepts -1

- **Full Backup**
  - Everything
  - Clear the Archive attribute
  - Weekly or any time major changes to the system are planned
  - **Backup takes longest, uses most space**
  - **Restore is fastest, fewest tapes required**

CISA
CYBER+INFRASTRUCTURE

**077 There are different types here, too. A full back up, for example, is everything across the enterprise. Now, it can be done, say, weekly, or periodically. You've got to think that through. And it's going to depend on how much data you're doing, how expensive it is, how much time it takes. These full backups usually take a long time. And they use up a lot of space. The good news is, though, if you're willing to go through that pain, they typically can get you restored pretty fast.

Backup Concepts -2



Backup Concepts -2

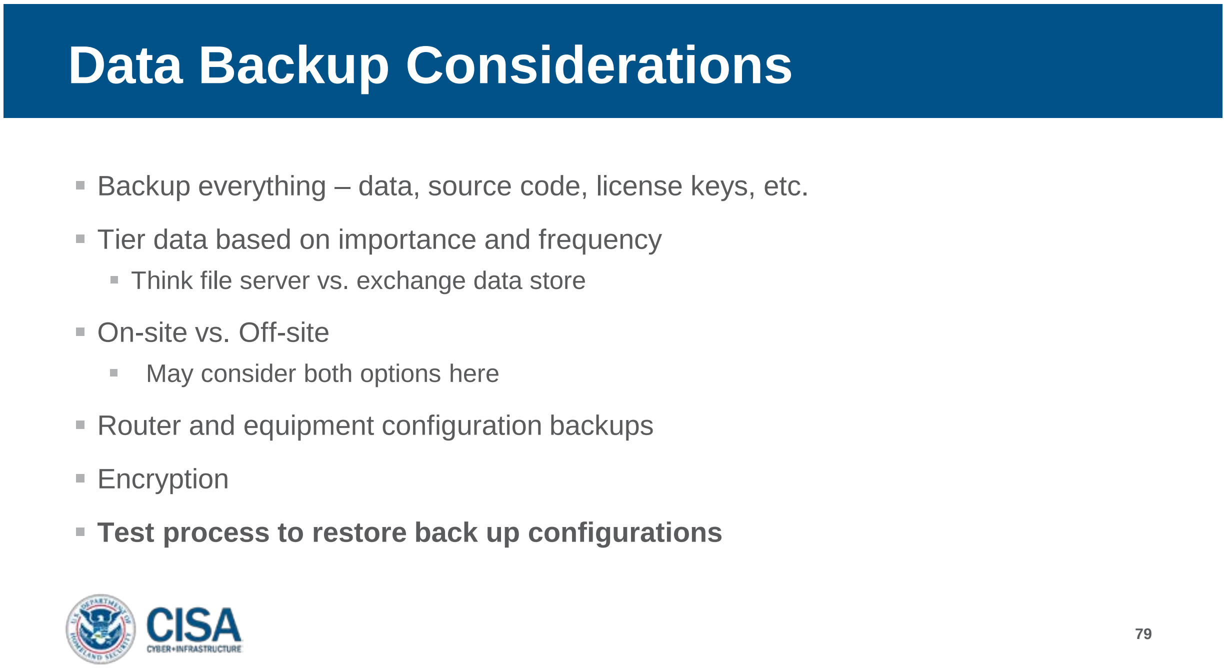
- **Incremental Backup**
  - Everything since the last full backup (files with the Archive attribute set)
  - Reset the Archive attribute
  - Require the **longest time and many tapes to restore**
  - **Fast backup** and requires the **least storage space** on the backup media
- **Differential**
  - Everything since the last full backup (files with the Archive attribute set)
  - DOES NOT reset the Archive attribute
  - Restore is **slower than full, but faster than incremental**, **less tapes required than incremental**

78

**078 Now, if you're not willing to endure that, you may want to use incremental backups. So, what you're going to do is you're going to take everything from your last full backup, and you're going to take pieces of it. This is going to take the longest time to do, and it's going to happen over a number of days. And to be honest with you, you may have a lot of tapes or memory space that you're going to be using to restore the site. If does provide relatively fast backup, but that said, it may not be nearly as good as a full backup.

You could also use a differential backup strategy. The thing to think about here is it is slower.

Data Backup Considerations



Data Backup Considerations

- Backup everything – data, source code, license keys, etc.
- Tier data based on importance and frequency
  - Think file server vs. exchange data store
- On-site vs. Off-site
  - May consider both options here
- Router and equipment configuration backups
- Encryption
- **Test process to restore back up configurations**

CISA
CYBER+INFRASTRUCTURE

79

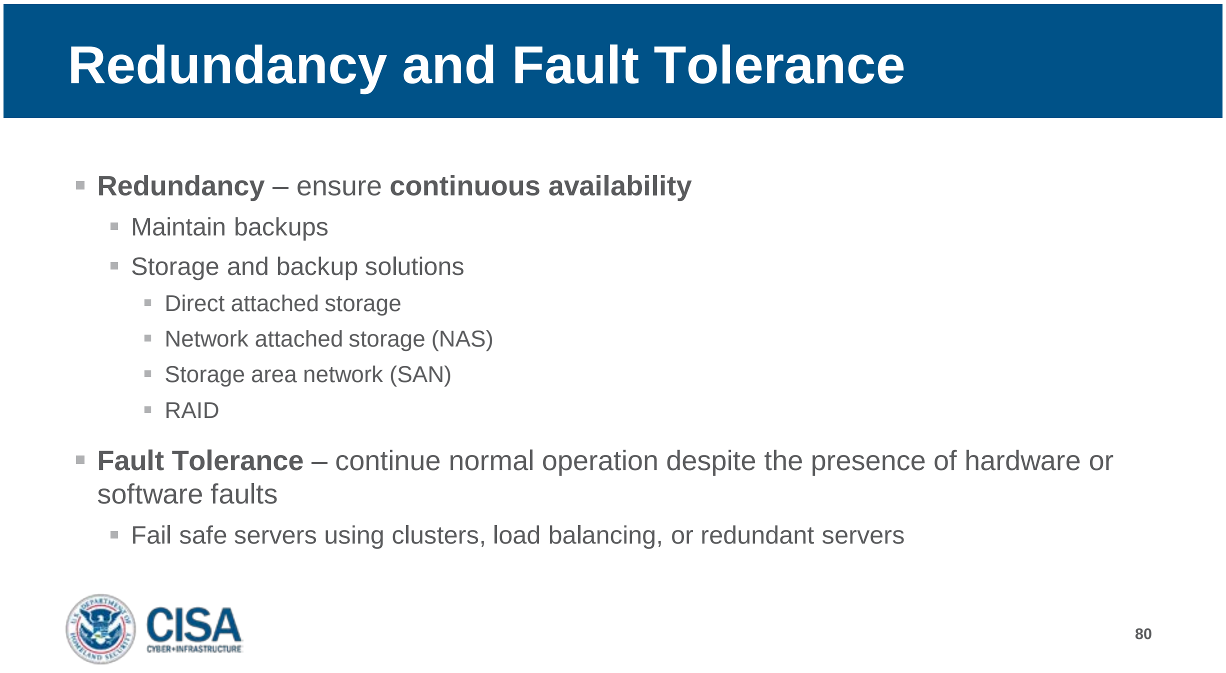
**079 Some other things you want to think about if you're doing data backups. First of all, make sure you back up everything. And when I say everything, you've got to think about even other remote systems that maybe are not as part of your network. Maybe you have separate networks in your organization. You need to start thinking about what data is on each and how you're going to store them. You're also going to want to think about if I'm backing up one and the other, do I ever let the two meet. In other words, am I going to back it up in the same system? Chances are, you may not want them to mix. You're going to want to think about what data is most important. And make sure you classify it in different tiers of prioritization.

How are you going to back it up also comes down to the where you're going to back it up. Is it going to be on site? Or is it physically going to be off site? You know, a good war story here is in an organization that I was once with, we were backing up our data off site. It was actually across town. And we worked with our service provider to make sure that we had a connection from our primary site to that second one. Well, one day, we lost connection from that site to the other. And we went back and reviewed the service level agreement. And we actually specified that we would have two independent connections to that off site facility.

What happened was a backhoe came through to do some roadwork. And it actually lifted two separate connections through the same trunk. It took out both connections to that site. So, we had to go back and review that service level agreement and specify that those independent connections had to be geographically separated as much as they were distinctly separate in and of themselves technologically.

You may also want to think about this information as I'm moving it. Does it need to be encrypted? Does it need to be protected somehow? And by the way, just like what we found out at this other organization, you need to make sure that you're testing the process so that way, if that darkest day comes, you know that the backup is going to actually work that's there.

Redundancy and Fault Tolerance



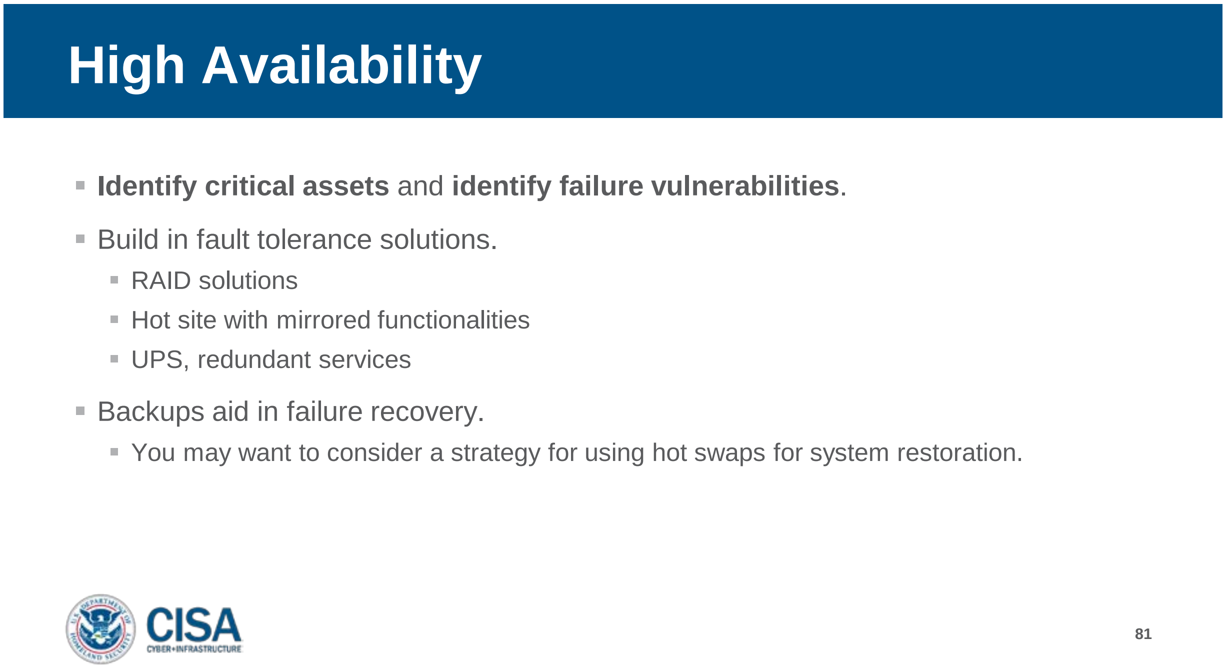
Redundancy and Fault Tolerance

- **Redundancy** – ensure **continuous availability**
  - Maintain backups
  - Storage and backup solutions
    - Direct attached storage
    - Network attached storage (NAS)
    - Storage area network (SAN)
    - RAID
- **Fault Tolerance** – continue normal operation despite the presence of hardware or software faults
  - Fail safe servers using clusters, load balancing, or redundant servers

80

**080 You may also want to think about how your system can be more redundant and how you're going to maintain these backups. Now, there's different strategies you can have here. Examples include direct attached storage through RAID. You also want to consider if you have a system maybe that's deprecated in capability that you may be able to withstand some of those faults and still operate. You need to understand the bounds of that. And if you can work with that fault tolerance, you need to make it work for you. You could do this through having clustered computer systems, maybe some load balancing or redundant servers.

High Availability



High Availability

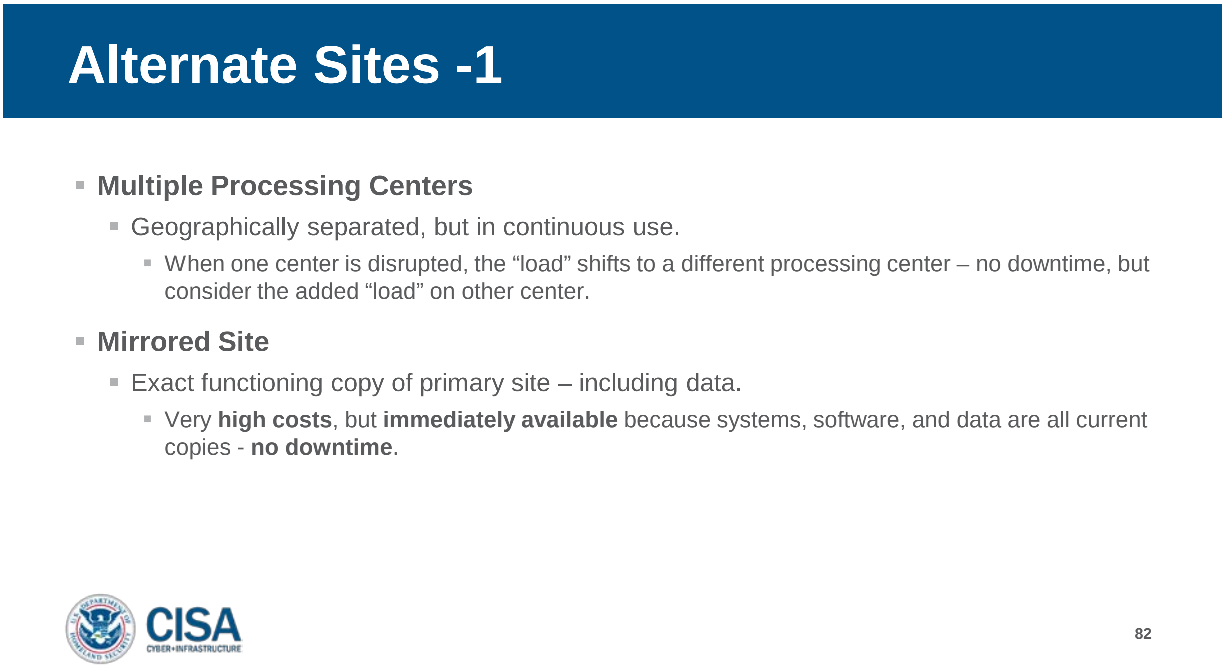
- **Identify critical assets** and **identify failure vulnerabilities**.
- Build in fault tolerance solutions.
  - RAID solutions
  - Hot site with mirrored functionalities
  - UPS, redundant services
- Backups aid in failure recovery.
  - You may want to consider a strategy for using hot swaps for system restoration.

CISA
CYBER+INFRASTRUCTURE

81

**081 You really want to go through and look at your high value assets and how they're delivering on your critical services because really what you need to know here is what needs to be most available. So, you're want to actually build in this notion of having fault tolerance in some of these systems. You're also going to want to look and see how your backups can help you in case you need to actually recover some of that information, at least pieces of it.

Alternate Sites -1



Alternate Sites -1

- **Multiple Processing Centers**
  - Geographically separated, but in continuous use.
    - When one center is disrupted, the “load” shifts to a different processing center – no downtime, but consider the added “load” on other center.
- **Mirrored Site**
  - Exact functioning copy of primary site – including data.
    - Very **high costs**, but **immediately available** because systems, software, and data are all current copies - **no downtime**.

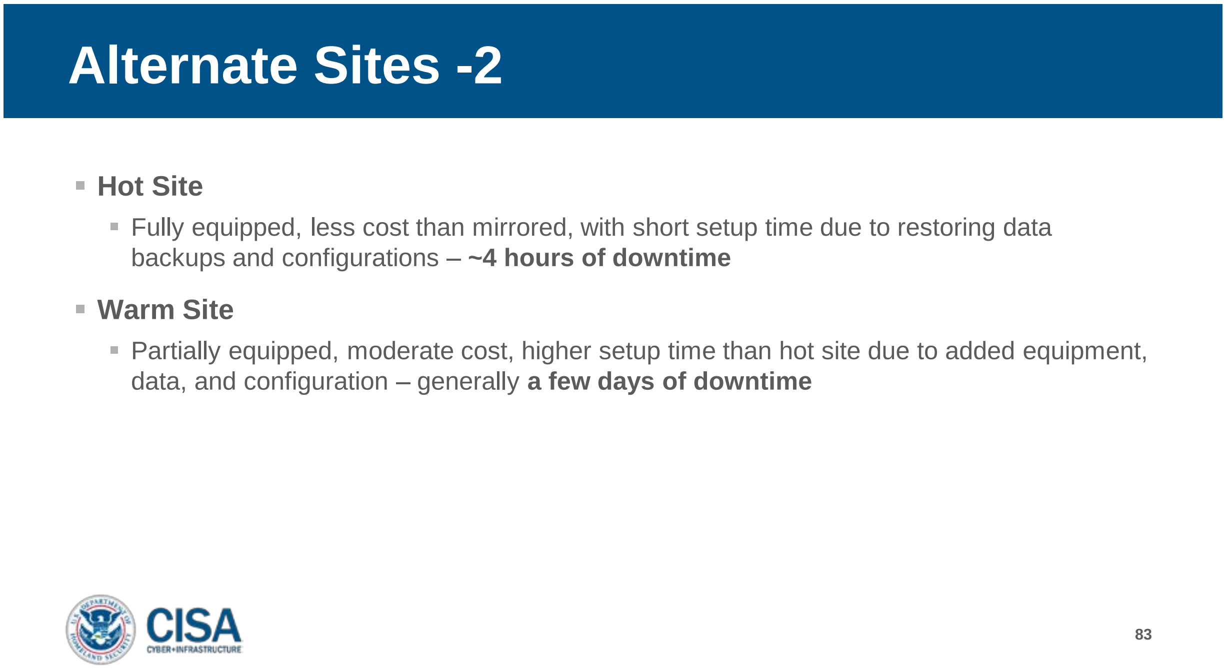
CISA CYBER+INFRASTRUCTURE

82

**082 So, remember, if your facility is taken out, you may actually have to go to an alternate site altogether to maintain your operations. There are some different terms here that we should understand. One is a multiple processing center type strategy. So, these are centers where you're actually conducting your processing at different geographic locations. And they may always be in continuous use. So, your load of your processing may shift from one to another. You want to make sure that that's as transparent as possible to the business, so it doesn't interfere with operations. And you also want to leverage it so that you can minimize your downtime.

You may also have a mirrored site. This is a little bit different. Think of another site across town that has the exact same functioning copy of what you have where you're resident. This includes the data that they have as well. Now, the problem with this one, it costs a lot of money and time and resources. But it helps you have immediate availability of your systems if you lose your facility. So, this means little to no transference in terms of downtime.

Alternate Sites -2



Alternate Sites -2

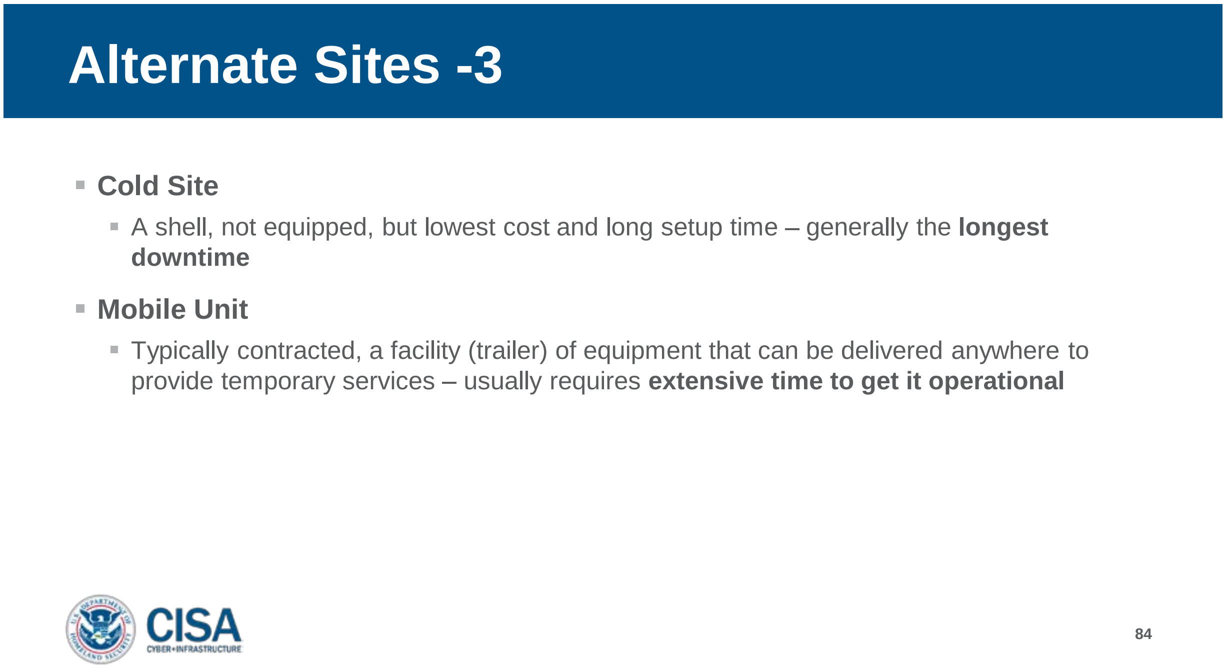
- Hot Site
  - Fully equipped, less cost than mirrored, with short setup time due to restoring data backups and configurations – **~4 hours of downtime**
- Warm Site
  - Partially equipped, moderate cost, higher setup time than hot site due to added equipment, data, and configuration – generally **a few days of downtime**

83

**083 You may also want to use a hot site strategy. Now, this is a-- basically, a room. It's going to be fully equipped with everything you have. Once again, maybe not across town, maybe another part of the world, geographically, somewhere that's easily accessible. This site may not be completely mirrored, but it will at least be set up to a point where it'll have a shorter set up time, typically about four hours or less.

This contrasts the idea of maybe you have a warm site. So, you now have a space that's partially equipped. And it's going to cost you maybe a little less, but now it may cost you in terms of how many days it may take to get back up. In this case, maybe a few days.

Alternate Sites -3



Alternate Sites -3

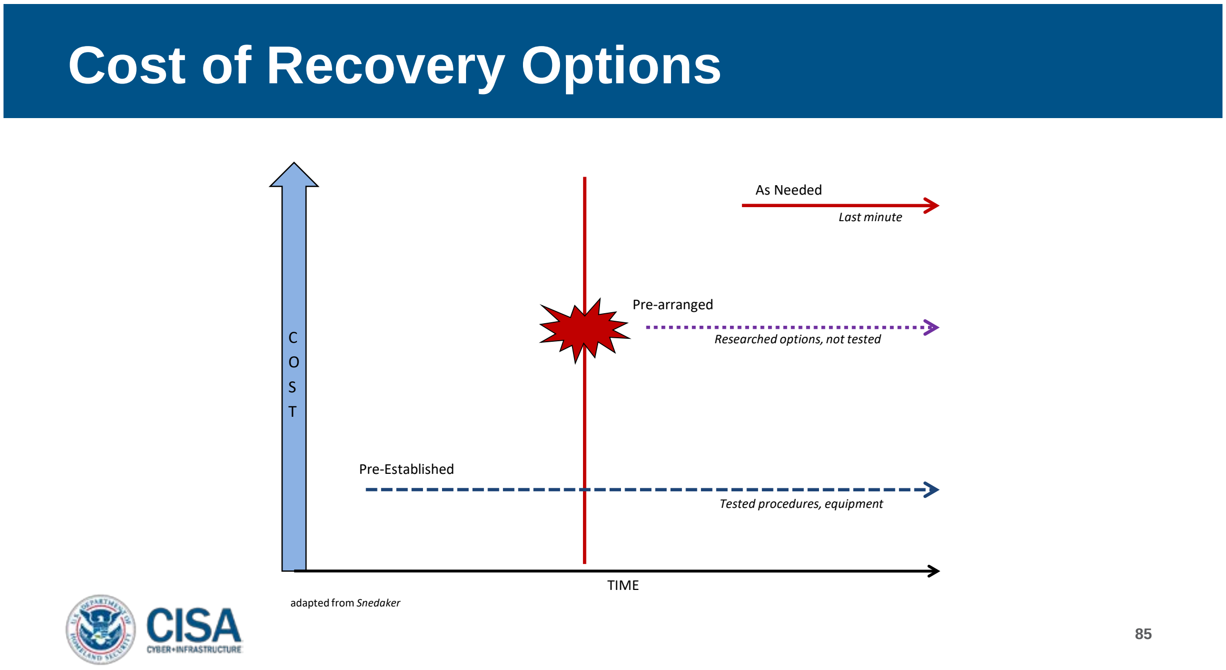
- **Cold Site**
  - A shell, not equipped, but lowest cost and long setup time – generally the **longest downtime**
- **Mobile Unit**
  - Typically contracted, a facility (trailer) of equipment that can be delivered anywhere to provide temporary services – usually requires **extensive time to get it operational**

84

**084 One other thought is you could have a cold site. Now, this is going to take obviously a long time to set up. This is literally just an empty space with walls and floor. You're lucky you have a roof with it. So, with this strategy, you really want to consider how you're going to fill this shell in a timely fashion such that you can get your operations up and running smoothly. What equipment are you going to want to get to that space? How fast? Does it have power? Does it have water? Does it have amenities so I can actually house people?

Another strategy is you may have a mobile unit. Think of a van or a truck that's carrying equipment similar in capability, maybe a little less, than what you have at your current site. The trick here is you have to keep it maintained and in an
area that's not local or resident to your immediate site.

Cost of Recovery Options



Cost of Recovery Options

As Needed

Last minute

Pre-arranged

Researched options, not tested

Pre-Established

Tested procedures, equipment

COST

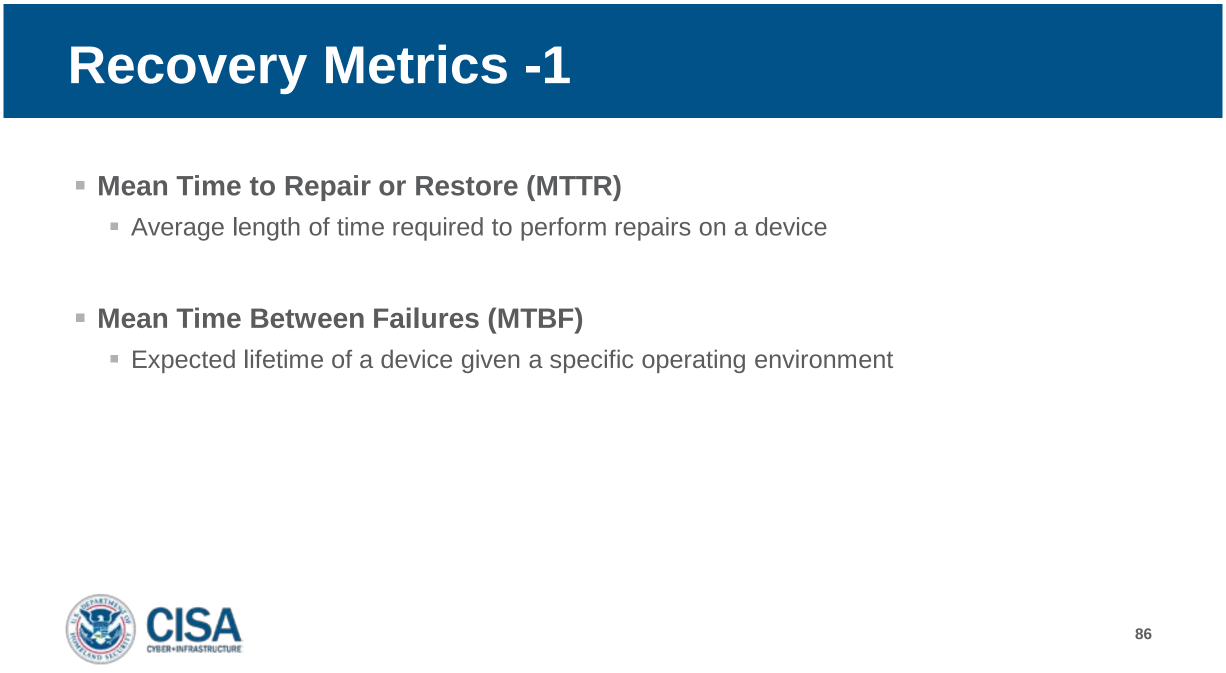
TIME

adapted from *Snedaker*

85

**085 Obviously, costs are going to vary depending on any of these operations. And this is going to become a key discussion area you have when you're selecting your strategy.

Recovery Metrics -1



Recovery Metrics -1

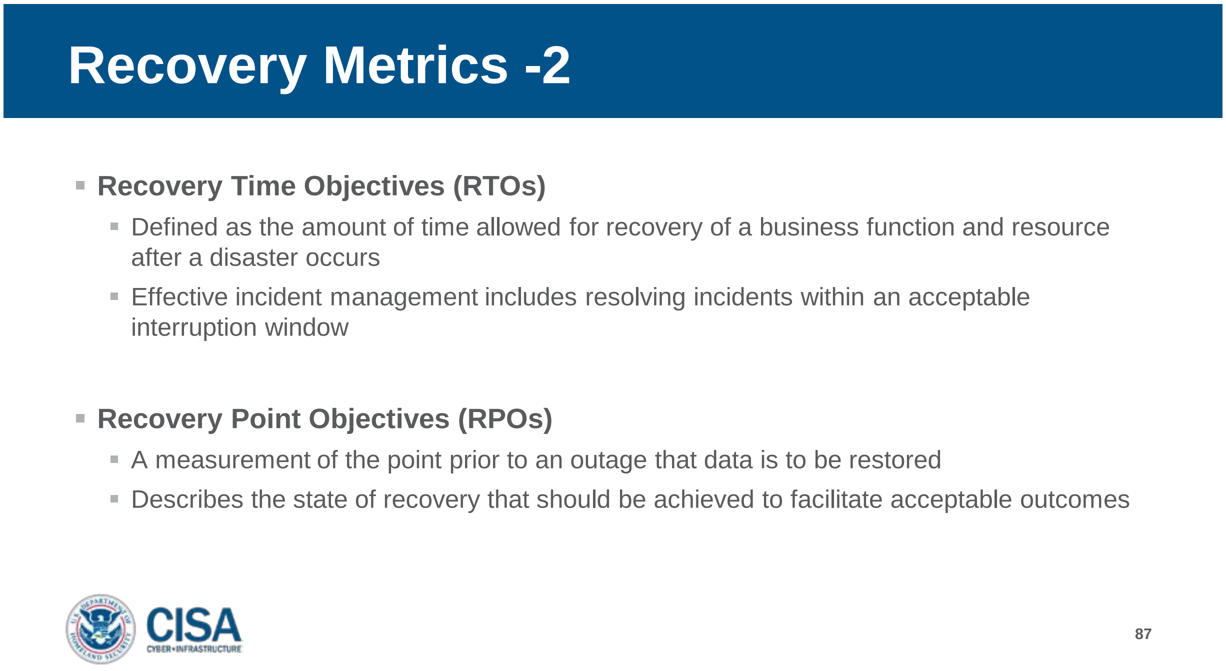
- **Mean Time to Repair or Restore (MTTR)**
  - Average length of time required to perform repairs on a device
- **Mean Time Between Failures (MTBF)**
  - Expected lifetime of a device given a specific operating environment

86

**086 Some ways that you can think about this, though, are revealing and looking at your metrics that you could have associated with this recovery. You can use these metrics to help you prioritize what solutions are going to be best for your organization. Suppose you use mean time to repair or to restore, MTTR. This is about the amount of time, the average length of time, that's necessary to actually get the repairs done, somewhat situationally dependent, but helpful at times, too.

You could also talk about mean time between failures. Now, this is the amount of time that a device has in a specific operating environment until it's expected to fail.

Recovery Metrics -2

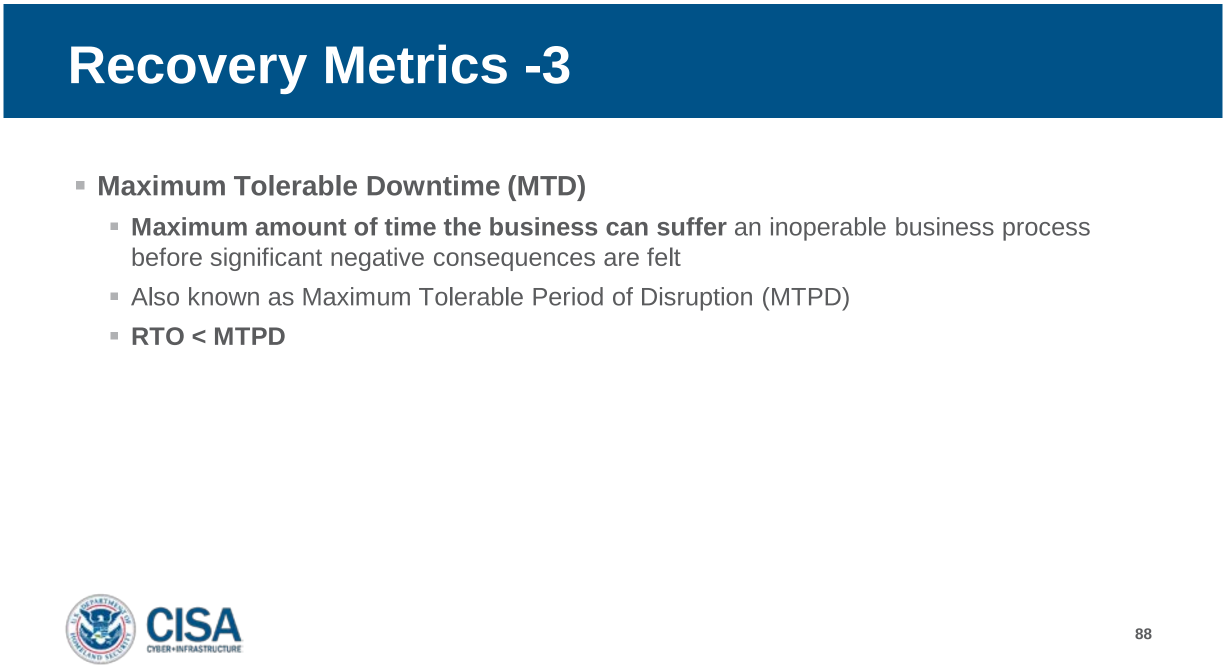


Recovery Metrics -2

- Recovery Time Objectives (RTOs)
  - Defined as the amount of time allowed for recovery of a business function and resource after a disaster occurs
  - Effective incident management includes resolving incidents within an acceptable interruption window
- Recovery Point Objectives (RPOs)
  - A measurement of the point prior to an outage that data is to be restored
  - Describes the state of recovery that should be achieved to facilitate acceptable outcomes

**087 So, another way to think about this, you may have an amount of time necessary to get back up and functioning. This is called your recovery time objective. You also may have a cutoff point where you have a notion as to where you want to restore your data from all the way up to the point of where this risk has been realized. That would be a recovery point objective.

Recovery Metrics -3



Recovery Metrics -3

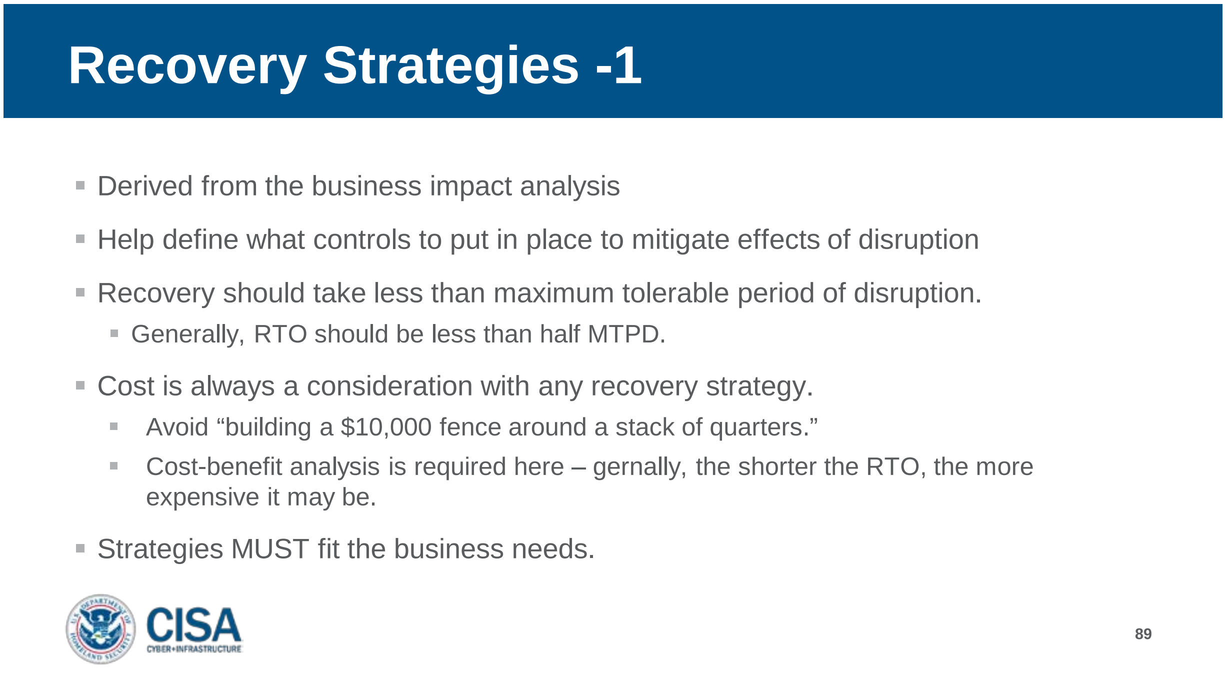
- **Maximum Tolerable Downtime (MTD)**
  - **Maximum amount of time the business can suffer** an inoperable business process before significant negative consequences are felt
  - Also known as Maximum Tolerable Period of Disruption (MTPD)
  - **RTO < MTPD**

CISA
CYBER+INFRASTRUCTURE

88

**088 In all cases, you may also have a maximum tolerance for the amount of time downtime that you can suffer in your organization and not feel as adverse an impact. This would be your maximum tolerable downtime.

Recovery Strategies -1



Recovery Strategies -1

- Derived from the business impact analysis
- Help define what controls to put in place to mitigate effects of disruption
- Recovery should take less than maximum tolerable period of disruption.
  - Generally, RTO should be less than half MTPD.
- Cost is always a consideration with any recovery strategy.
  - Avoid “building a $10,000 fence around a stack of quarters.”
  - Cost-benefit analysis is required here – gernally, the shorter the RTO, the more expensive it may be.
- Strategies MUST fit the business needs.

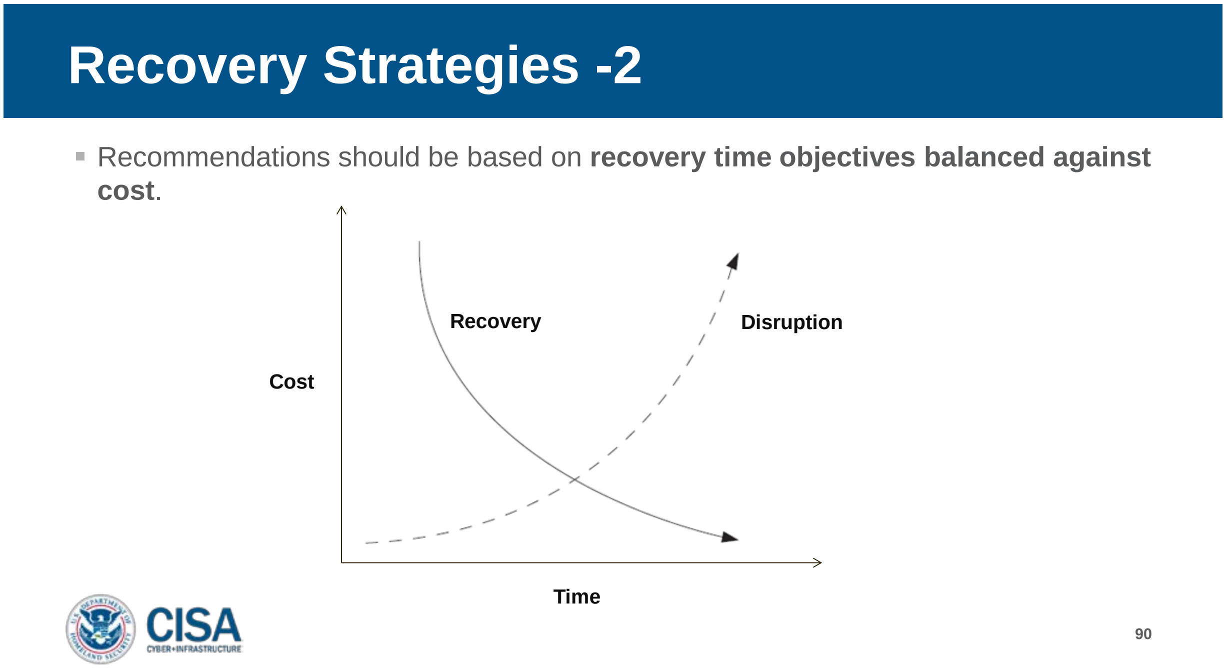
89

**089 So, there are some different strategies that you can go through here. And typically, what you want to do is you want to go through a business impact analysis and understand how your organization is going to feel the pain. Let's start from the beginning here a little bit. Remember, what we did is we understood our critical services. And from those, we understood what assets were necessary to support those services. Then we define what the risks are. And remember, risk is nothing more than uncertainty that has an element of threat, vulnerability, and an impact related to it.

When we went through that analysis, we really needed to understand how we were going to feel pain if that risk were to be realized. You're going to want to bring that information to the table as you're developing this recovery strategy. You really want to know, too, what controls you're going to be putting in place to mitigate these effects. And you want to be proficient in understanding how they're implemented, especially for the people who are actually implementing, your incident response team, for example.

Now, clearly, what you want to do is you want to get your operation back up and running in less time than what you can tolerate. So, generally, you want your recovery time objective to be less than your mean time to failure. As we think about this, cost is always going to be a consideration. There's only so many resources you can put to this. This goes with the old adage that you don't want to build a ten-thousand-dollar fence around a stack of pennies or quarters. So, really, this is where your cost-benefit analysis is going to come in handy so that way you know your risks are being addressed, and it's not breaking the bank. In all cases, you have to fit your business needs.

Recovery Strategies -2



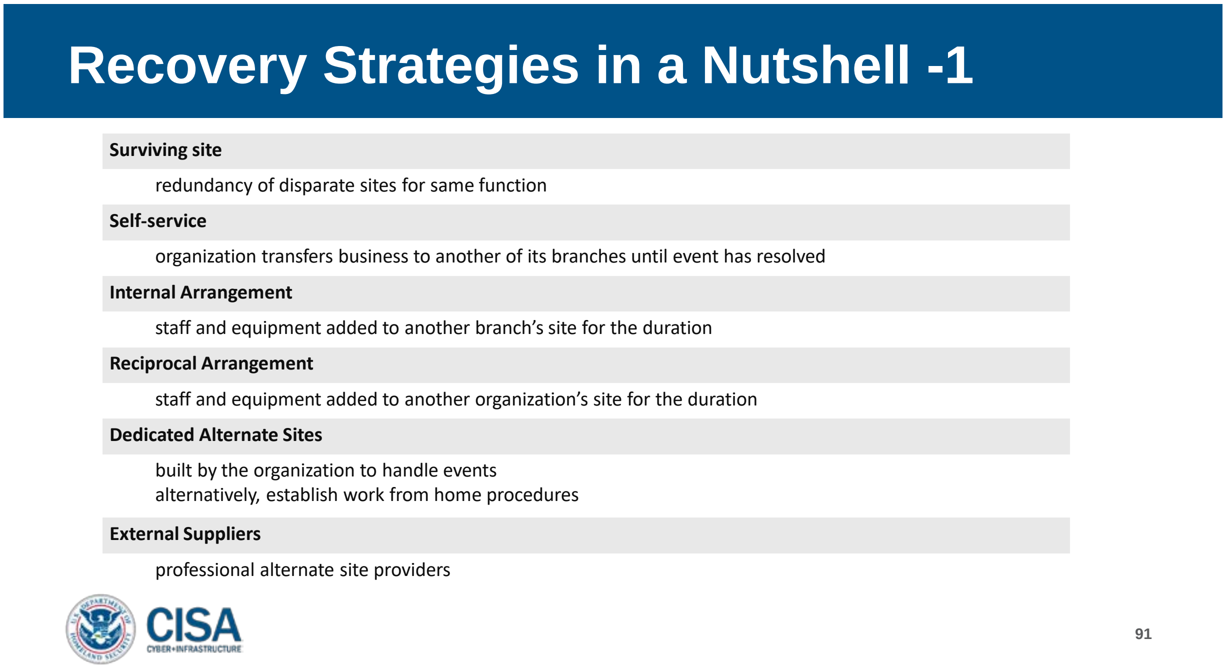
Recovery Strategies -2

- Recommendations should be based on **recovery time objectives balanced against cost**.

90

**090 If you want to think about this graphically, what we can do is we can balance our recovery time objective against the costs that we're going to be investing.

Recovery Strategies in a Nutshell -1



Recovery Strategies in a Nutshell -1

Surviving site

redundancy of disparate sites for same function

Self-service

organization transfers business to another of its branches until event has resolved

Internal Arrangement

staff and equipment added to another branch’s site for the duration

Reciprocal Arrangement

staff and equipment added to another organization’s site for the duration

Dedicated Alternate Sites

built by the organization to handle events
alternatively, establish work from home procedures

External Suppliers

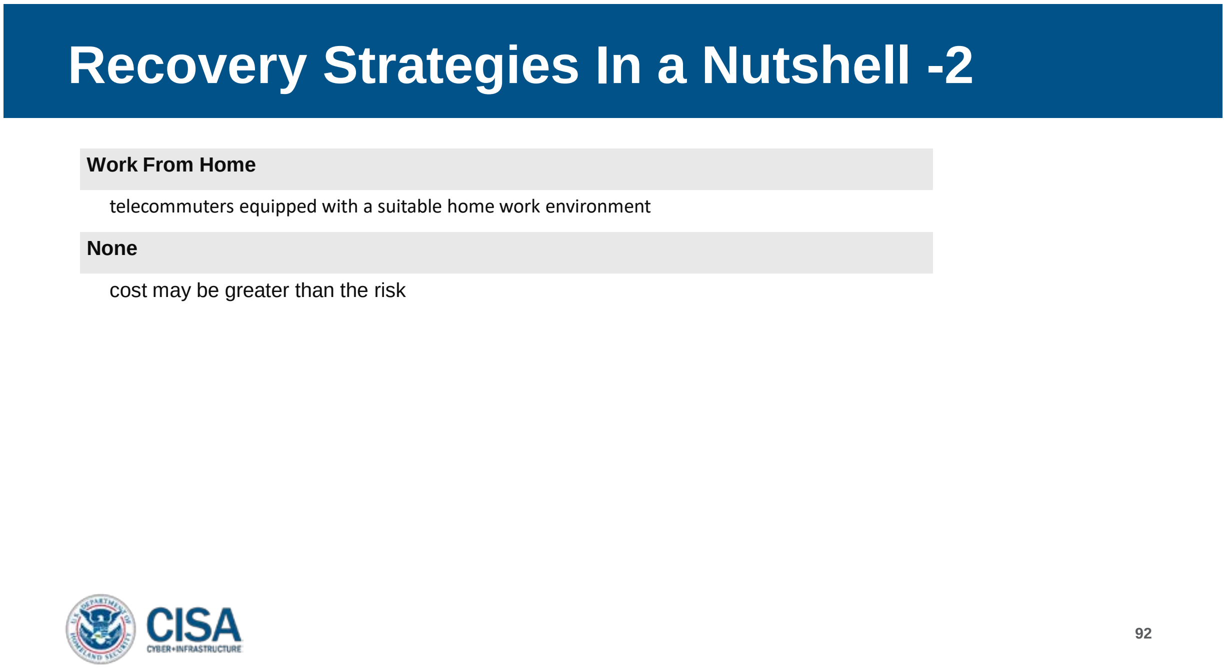
professional alternate site providers

91

**091 So, in a nutshell, what we want to think about here, you want to be in consideration of redundancy of your surviving site despite what may happen. How is it that you're going to keep that same function? Maybe your organization is one that's based on self-service, and you can move that service around to other branches, and they can actually do the work for you. Maybe you have an internal arrangement where you're going to go share space with other pieces or other members or pieces of your organization that's existing. Or maybe even work outside your organization, and you have reciprocal agreements where you're going to actually, let's say, down the street and work with a whole other company. Now, in these cases, clearly, it's going to be for a certain duration of time. What you're going to want to do is negotiate this ahead of time, so there's an understanding as to how long you're going to actually be resident with them.

You may also, as we've talked before, have dedicated alternate sites. This is the whole hot site, warm site, cold site discussion. You're going to know where those are at and the procedures and the logistics to get there. You may also have agreements with your external suppliers. They maybe able to help you in these times of need, as well.

Recovery Strategies In a Nutshell -2



Recovery Strategies In a Nutshell -2

Work From Home

telecommuters equipped with a suitable home work environment

None

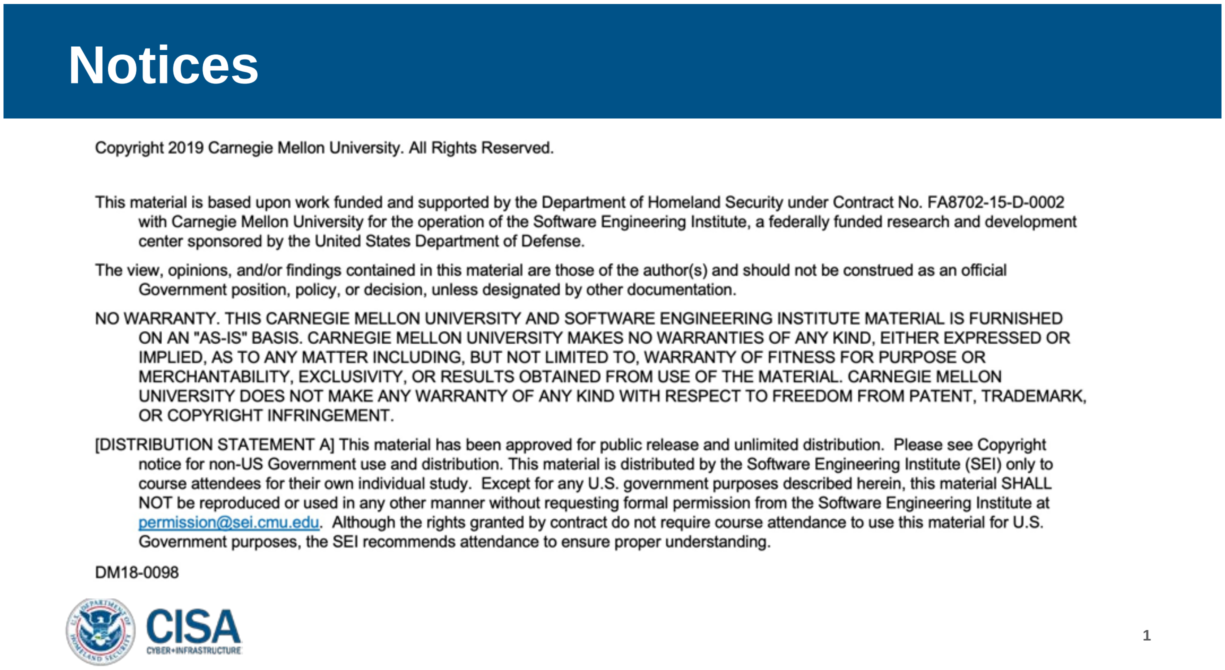
cost may be greater than the risk

CISA CYBER+INFRASTRUCTURE

92

**092 Some other strategies to consider, imagine if you have an issue where your facility has burned to the ground. Maybe you have a communications plan in place where you just call your employees and say work from home. Good thing everybody takes home their laptops. Now, by the way, that's a matter of culture. If, in fact, you have this work from home strategy operating, you're going to clearly want to tell your employees to continually take home their laptops if possible. By the way, there's always the possibility that you may actually decide to not do anything, clearly, the cheapest path to take, but also the riskiest.

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.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM18-0098