# Administrative Controls

## Table of Contents

# Common Administrative Controls

- Policies and Procedures
- Personnel Policies
- Passwords Policies
- Service Level Agreements (SLAs)
- Security Related Awareness and Training
- Change Management
- Configuration Management
- Patch Management
- Archival, Backup, and Recovery Procedures


CISA CYBER+INFRASTRUCTURE

27

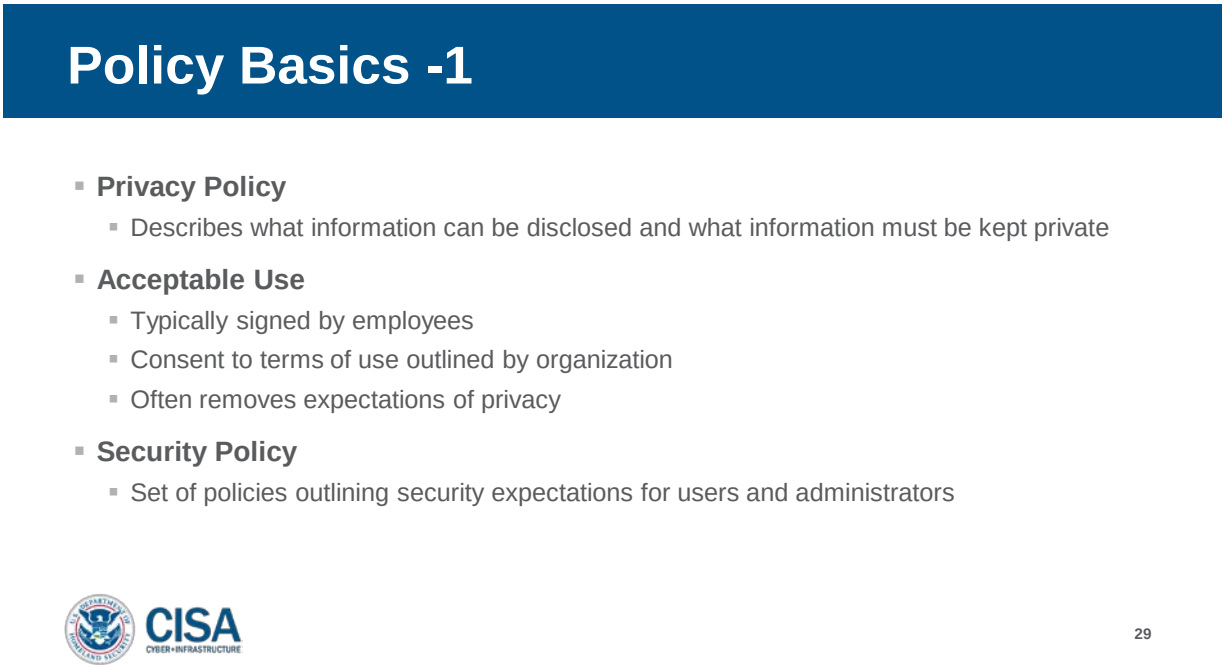
**027 Instructor: We have an exhaustive-- not necessarily an exhaustive list, but it looks like a long list of different administrative controls that we can put in place. Let's talk about these a little bit, each one at a time.


**028 For example, we could actually just establish policies and procedures. Policy is like a direction that you give the organization. It really expresses what the executive management's desire is for the organization to follow rules. It sets a tone, and it should be a tone at the top, by the way, for how operations should take place. It's actually, if you think about it, a cultural instrument, because it sets the backdrop for how an organization's going to operate.

Now, some of these policies may be applicable globally to an entire organization, or you may have local policies that apply. Also you want to think about who is going to approve the policy, who reviews it, how often is it reviewed. How well is it written? Is it written for people who are of

maybe a different background or culture to understand it?

### Policy Basics -1



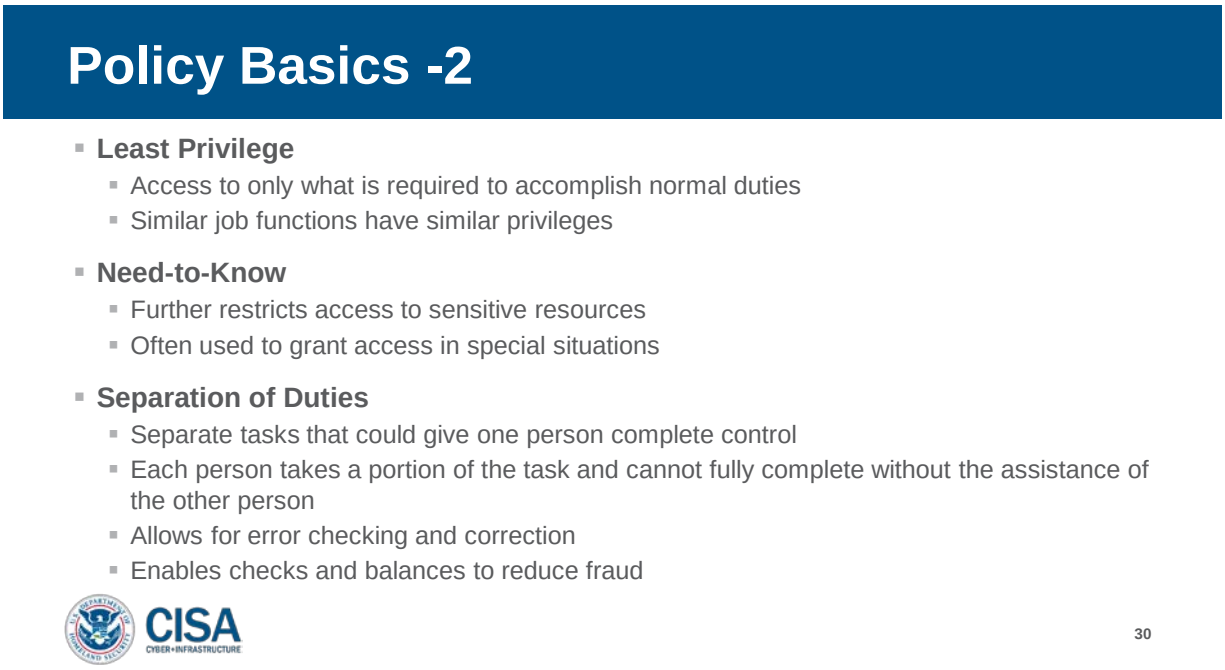

**029 There are different types of policies you may want to consider here when it comes to cyber risk management. For example, you could have a privacy policy, and this could really go back to what needs to be kept private in terms of maybe personal information, for example.

You may have an acceptable use policy. This is especially important if you get new people in the organization and you have employees who really need to know what are the bounds of what they're allowed to surf on the internet over lunch, for example. You may actually have training associated with that. You may actually have them sign a document so that they understand

that they know what the acceptable use of your organization's assets are.

You could also have security policies, and these are going to actually gauge and determine what's expected of now only employees but maybe of administrators and what they're actually supposed to do in terms of controlling your systems to make sure that there's no malicious activity that takes place on your systems.

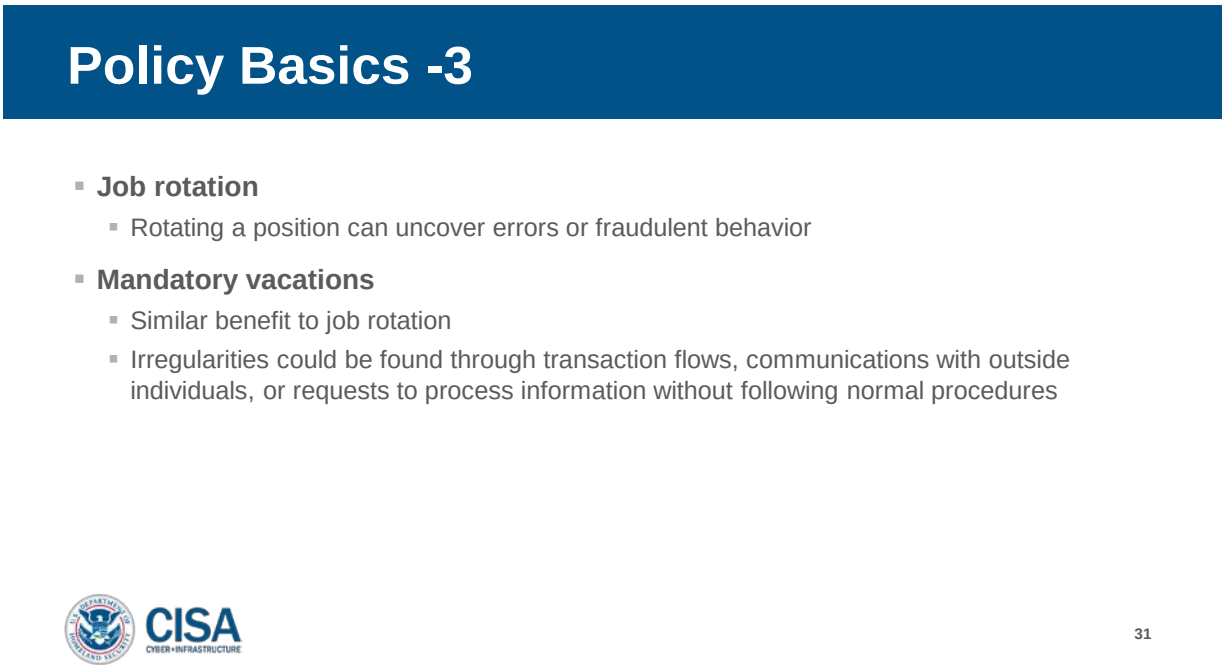
### Policy Basics -2




**030 You could have a least privilege policy. This is where we're actually determining what the access to these systems are. It may also depends on who has a need to know, and you may document that in yet another policy. You may also want to determine who gets what access depending on what duties they have.

Now, what you really want to do here is make sure that you have the duties separated such that no person can accrete the information in one spot and cause the greatest amount of damage to your organization or your assets. So you're actually going to separate the duties and give them separate needs to know, for example, so that way they can still execute their job but they only have a certain data set to do it with.

### Policy Basics -3

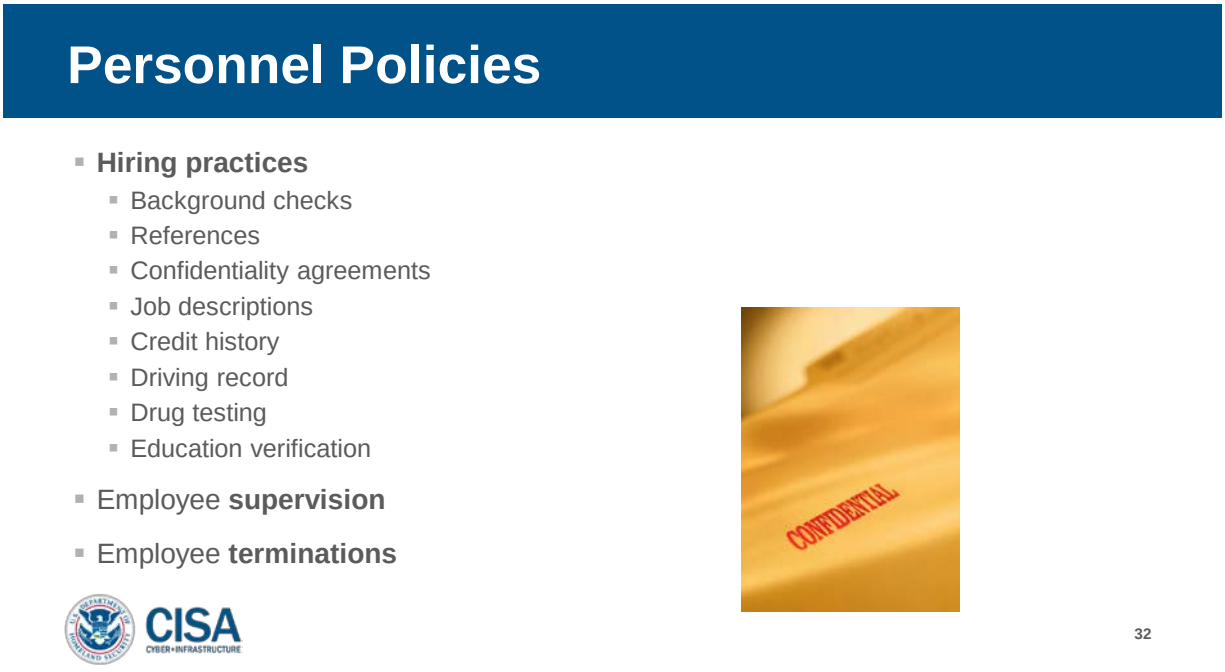



**031 You may also want to think about job rotations. So in this particular case, if we have a person that's in a particular role and that role has the ability to create a certain amount of mischief in an organization, or maybe bring an organization to its knees in terms of what kind of damage that can be done-- maybe the level of

confidentiality is really high with that particular job, maybe integrity's really important-- you can actually make it so that people actually have to rotate in and out of that job so that way you keep them off balance and you can identify fraudulent behavior if it's taking place.

You can also enforce mandatory vacations. Make people go away for a while, and maybe you will start to see that transactions will change, or the communications inside or outside the organization will change, and this may be indicative of a negative trend in the organization, of people not following a procedure, for example.

### Personnel Policies




**032 We may also want to think about personnel policies in an organization. We've already talked about the idea that people are

absolutely critical to our organization, but to be honest with you, they actually have great power to bring an organization to its knees as well if you're not careful. So you want to think about this before you even bring them onboard. Think about your hiring practices. Are you doing the background checks necessary to understand where they're coming from, to make sure that they have not partaken in any criminal activity prior to coming to your organization. That may be indicative of future action. You may also think about references and checking any references to see their previous performance at other organizations.

You may also have them sign confidentiality agreements so that they don't expose proprietary information without at least have the sense of significant penalty coming against them if they do so.

You can separate their job duties by having very detailed job descriptions for them. This will all come back to that need-to-know idea as well.

You can investigate their credit history. You can look at maybe their driving records. Now, by the way, driving record is not going to be as much of an issue. This is going to be for someone who maybe is in your organization that is also doing driving or maybe some kind of shipping and delivery for yourself.

You can also look into their resume to validate that they have the

education that they said that they have.

You want to keep in mind too how you're supervising your employees, because let's face it, you don't quit a business, you quit your boss, and a boss can easily set the tone for a negative environment where you may have insider threat become a risk. You may also want to think about how you're terminating your employees and moving them out of the organization. Are you securing their access to their accounts in a timely fashion such that they can't take information and/or do something malicious before they're terminated?

### Passwords Policies

## Passwords Policies

- **Password** policies are a must!
  - Complexity – upper and lower case, numbers, and special characters
  - Length
  - Age
  - Account lockout and reset
  - Auditing
- User **training and awareness** is important.
  - Include password best practices in security training.
  - Provide examples of good and bad passwords.


CISA
CYBER+INFRASTRUCTURE

33

**033 You may also establish policies around how passwords are set up in your organization, and we

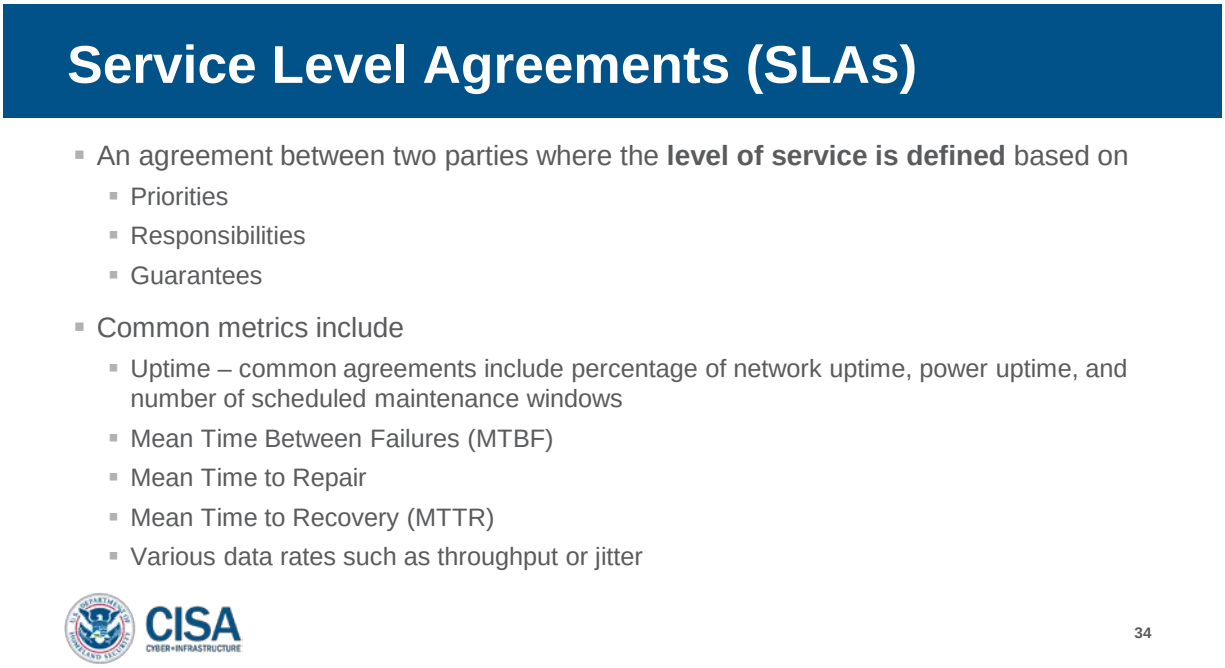
all do this-- we're all logging into our computers at one point in a day or another, and when we do that, we put a password in, and obviously we do it so often that it may be even just second nature. Some people though tend to write their passwords down. This is especially true when you have an organizational policy that demands a lot of complexity-- something to keep in mind. You have to balance it. The length would also be a possible issue there. You may also want to think about how long they're allowed to keep a certain password.

Now, you can also set your system so that it looks for the complexity of the password changing over time. You don't want to have someone use their pet's name and 01, pet's name 02, pet's name 03 the next month. So you're going to want to look at that as well.

You're going to also have policies set around what actually brings out a lockout in a system. Would it be three negative logins? Maybe they would have to actually go to an administrator and have their system-- to have their access reset altogether. And you're going to also want to audit to make sure that people are actually following these password policies as well. You also want to make sure that they're aware of the responses in establishing proper cyber hygiene in terms of password development.

A good idea is to provide examples--good passwords, bad ones, and what is allowed in the system and what's not.

### Service Level Agreements (SLAs)




**034 You also have to focus on how you establish service- level agreements. Remember that these are agreements that you establish with other organizations so that way you get the services rendered that you're paying for. You got to be careful here because you want to make sure that the agreement is constructed in a sense that you're getting the exact scope of what you're paying for. You have to think about what you have priority in in terms of getting a return for your resource there. You want to think about the responsibilities that that organization has for you. And by the way, you may have to dictate priorities of what actions you want

them to take for you as well, and you actually may even want to incorporate some guarantees. "You will be guaranteed to deliver me X services if a certain event happens," for example.

You may want to look at different metrics to measure how that third-party is performing for you. So let's say they're providing a service where a piece of equipment has to be up for a certain period of time. You may also want to think about how often their equipment is failing. How long does it take for them to go from repair back to full operation? How long does it take for them to recover operation if they were to lose it? These are all things that you may want to specify in that service-level agreement.


**035 You also want to be sure to keep training your employees and keep them aware of your policies. A good example of this could be your data classification and privacy policy. If you have employees that are dealing with HIPAA information, health-related information, for example, you want them to be very aware of what they're working with and the high level and degree of responsibility that they have for that information. So with that awareness, you're going to teach them how to actually handle that information and how to keep it secure.

You're going to also want to focus on their habits. This is where cyber hygiene may come into practice. You want to make sure that people are doing the right things on your system so that way the information that they

have on that system cannot be corrupted.

You may want to also keep your employees aware of certain threats that may be in an environment. Maybe it's the fact that you have-- as a gross example-- someone loitering outside your organization on the campus, and you don't really know what their purpose is there. That would be a gross example of a physical threat awareness. But it may also be the idea that you have a phishing email that comes into your organization. That in itself could be a new threat. So you may somehow advise your employees that you have this phishing email going around the organization and you give them a warning not to open it up.

# Archival, Backup, and Recovery Procedures

- Information should only be kept as long as it is required.
- Generally, recovery will take longer than backup.
- Practice recovery.
  - Test your procedures.
  - Test your backups.

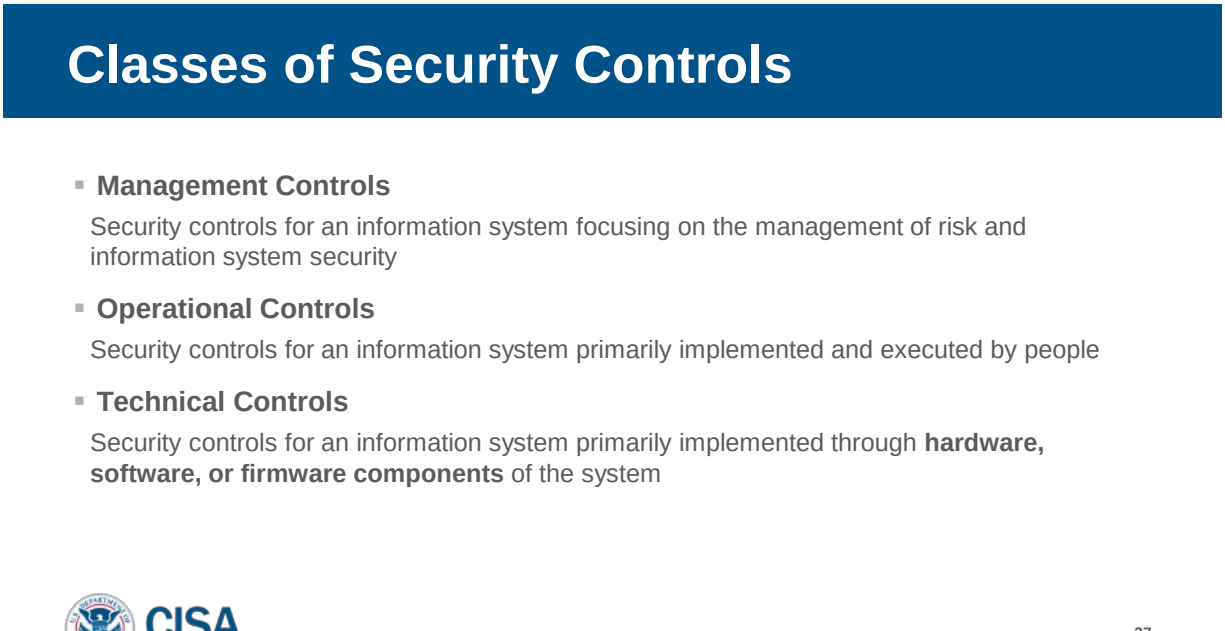

CISA
CYBER+INFRASTRUCTURE

36

**036 Some other examples of some procedures we may have are archival backup and recovery procedures. Now, what we want to think about here is the fact that our organization has, for whatever reason, fallen into a bad time where we actually have lost the integrity and/or the availability of information that we were using to make our organization go. So what are we going to do? We're going to be backing up this information and we're going to have it on a separate system altogether so that way we can come back, recover that information, and get back into the game. And by the way, this is not easy. There are all different types of technology we could talk about here, and there's also this notion that even though you had that technology, you need to test it. You need to make sure that it

works for you, not just physically and technically that it's actually happening, but the people who are operating and have to actually make sure that they're doing the backup correctly and that they're doing the recoveries correctly-- you have to make sure that they know what they're doing as well.

### Classes of Security Controls

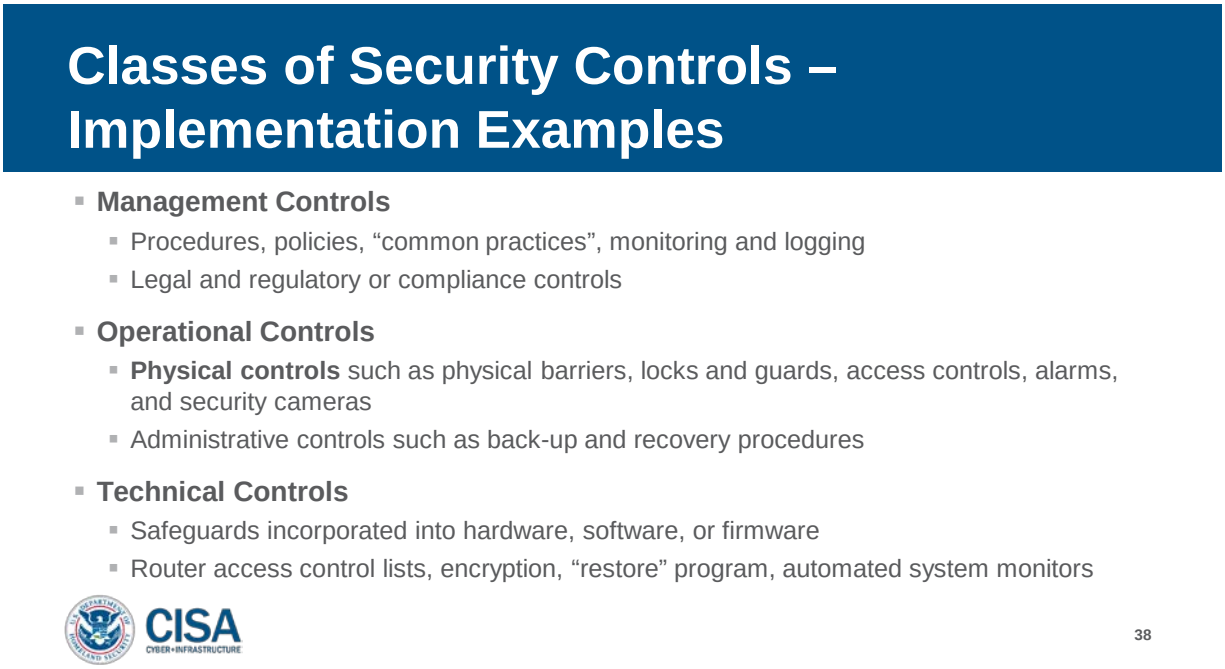



**037 So now let's talk about classes of security controls, because there are different types, and I want to decompose these eventually too into specific examples.

First you may have management controls. These are controls that actually focus on the management of risk in the organization, or within your information security system. You may have operation controls, and this may control literally how

people are doing things day to day. You may also have technical controls, and these are controls that are found in your computer systems. A good example here would be any hardware or software that you've installed such that it prevents malicious actors from getting in.

### Classes of Security Controls – Implementation Examples

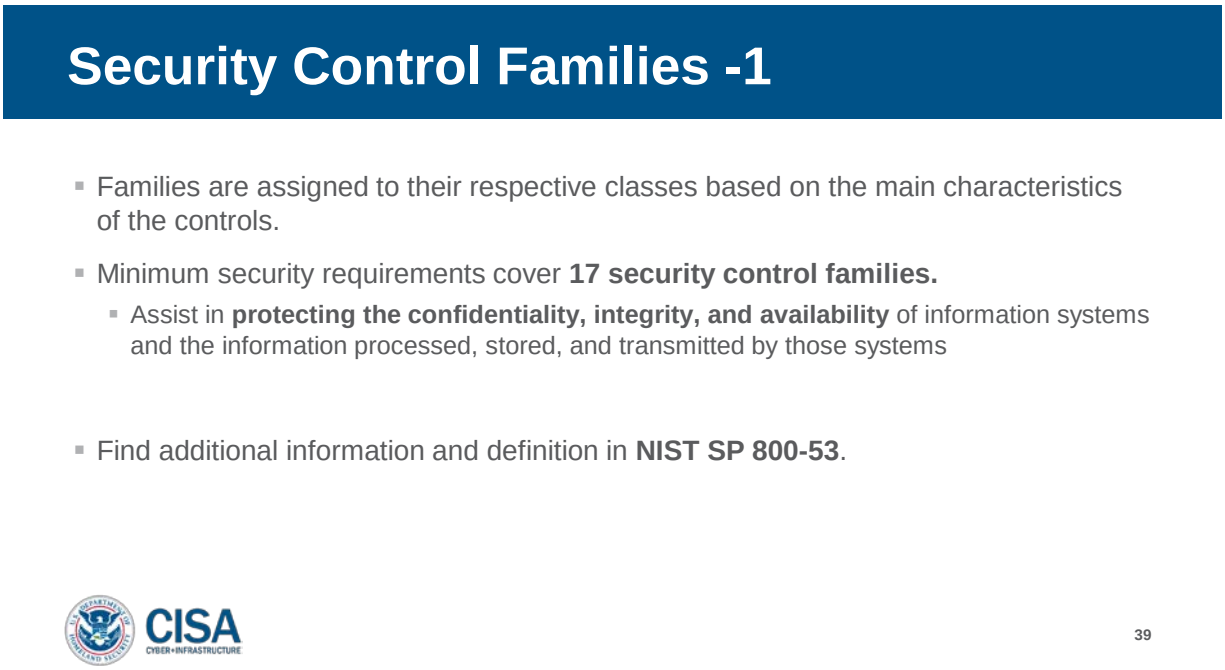



**038 So let's give some examples of what these may be. Management controls, for example, could be policies, procedures, maybe even some common practices. We may even have some regulatory compliance controls that we're following.

Operational controls could be physical ones. Remember we talked about locks, guards and gates, access controls? Those are examples of operation controls.

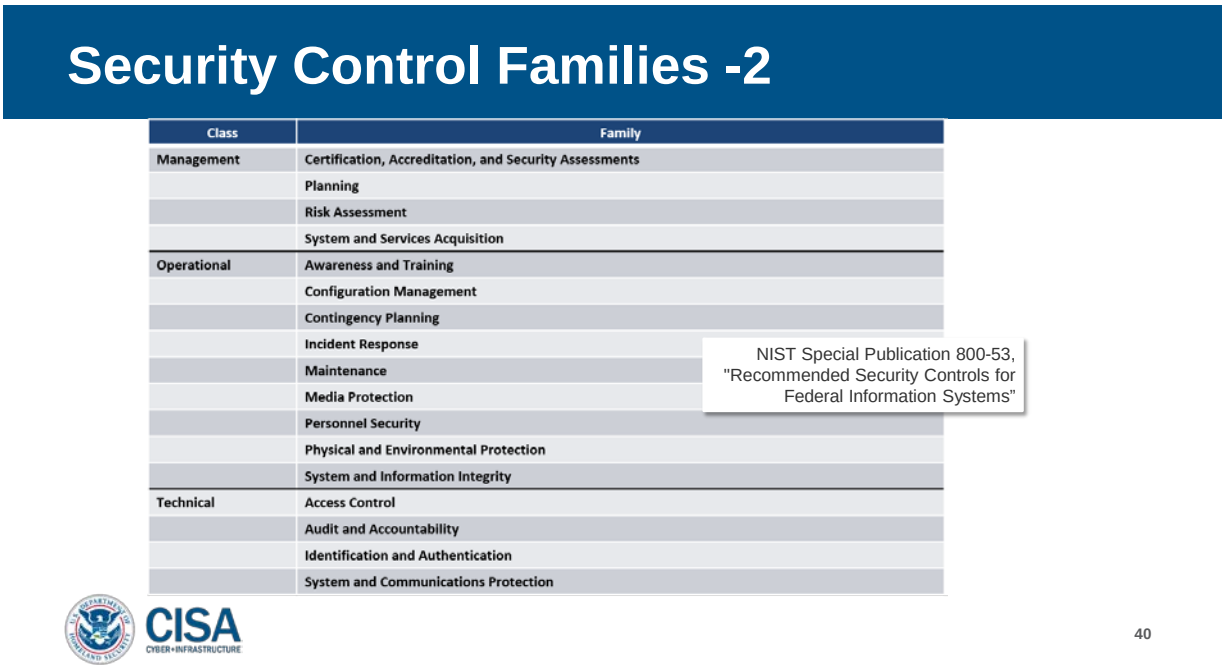
They may also be administrative. Maybe we have backup and recovery procedures. Technical controls would be what we have on our systems. So these are safeguards that we may have in terms of our hardware or software. We may have router access controls, for example. We may have certain data that's encrypted.

### Security Control Families -1




**039 So what I want to do is familiarize you with NIST SP 800-53, and within it, it talks about security control families. There are 17 of them, and they're all geared toward that CIA framework-- confidentiality, integrity, and availability-- and how we protect it.

## Security Control Families -2



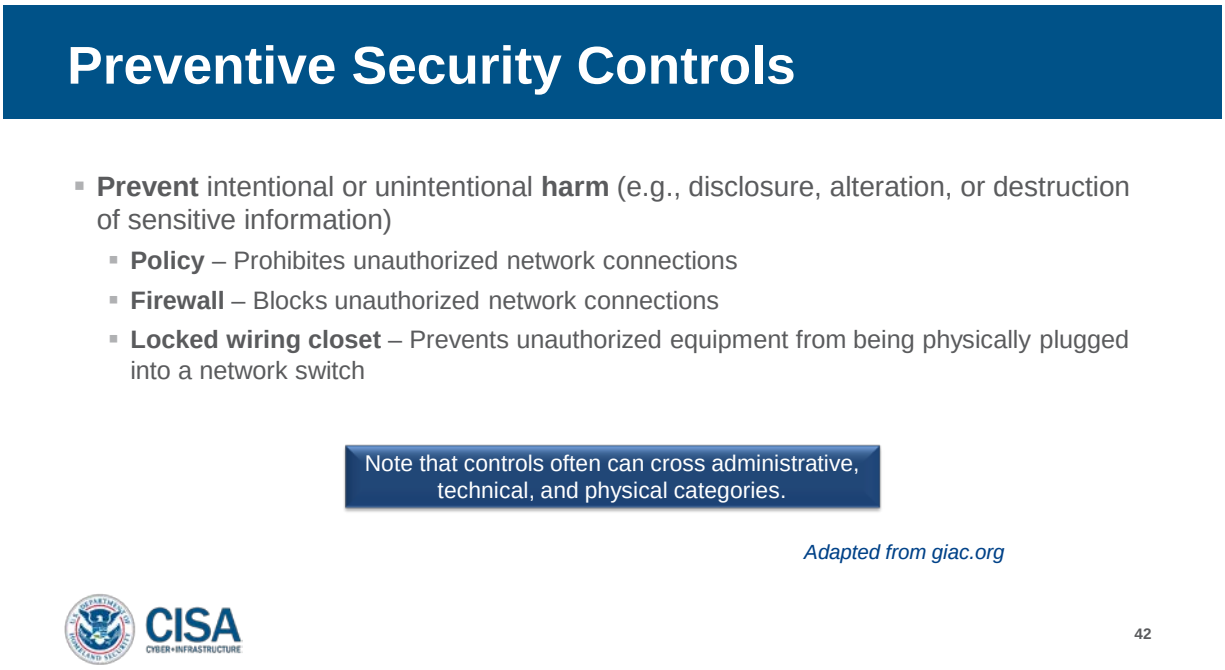

**040 Here's a slide that summarizes them for you. I'm not going to go exhaustively into each of these, but I would welcome you to go to NIST 800-53 and review each of these because there is a lot of detail here that NIST 53 provides. I would like to note that the management, operational and technical classes are broken up into families, and within those, you'll find controls under each of those families as well.

# Control Categories

- There are many different control categories **based on the intent** of the security control **and its effect** on risk.
  - Prevent
  - Detect
  - Correct
  - Recover
  - Direct
  - Deter
  - Compensate



**041 Let's talk a little bit about how we're going to categorize our controls. Now we can do this based upon the intent of what we're trying to do with each of them. For example, we could have controls that prevent malicious actions from taking place, versus ones that actually just detect. Let's go down the list in a little bit more exhaustive manner here.




**042 For example, we have preventive security controls, and what we do with those is we want to prevent intentional or unintentional harm. We can do this by establishing policies that maybe prohibits access. We could have maybe firewalls set up in a system to prevent access. We could have locks on equipment so that way people can't get in.

# Detective Security Controls

- Like a burglar alarm, they **detect and report** an unauthorized or undesired event or attempted event.
  - Log monitoring and review
  - System audit
  - File integrity checkers
  - Motion detection


*Adapted from giac.org*

CISA CYBER+INFRASTRUCTURE

43

**043 We could also have detective security controls, and these are to basically see what's coming and going. We can monitor logs of what's taking place in our systems. We can do audits on our systems. We can also, from a physical aspect, we can have just motion detection so that way we can see people coming and going in our facility.


**044 We can have corrective security controls. Some examples here would be maybe we have a procedure to actually take a virus out of the system once it's infected the system. It's something that we're doing to actually fix or remedy an incident that has already happened, and what we're really trying to do is reduce further damage. Another example could be physically a guard checking to look to see that the facility is clear of any intruders if a door is left unlocked.

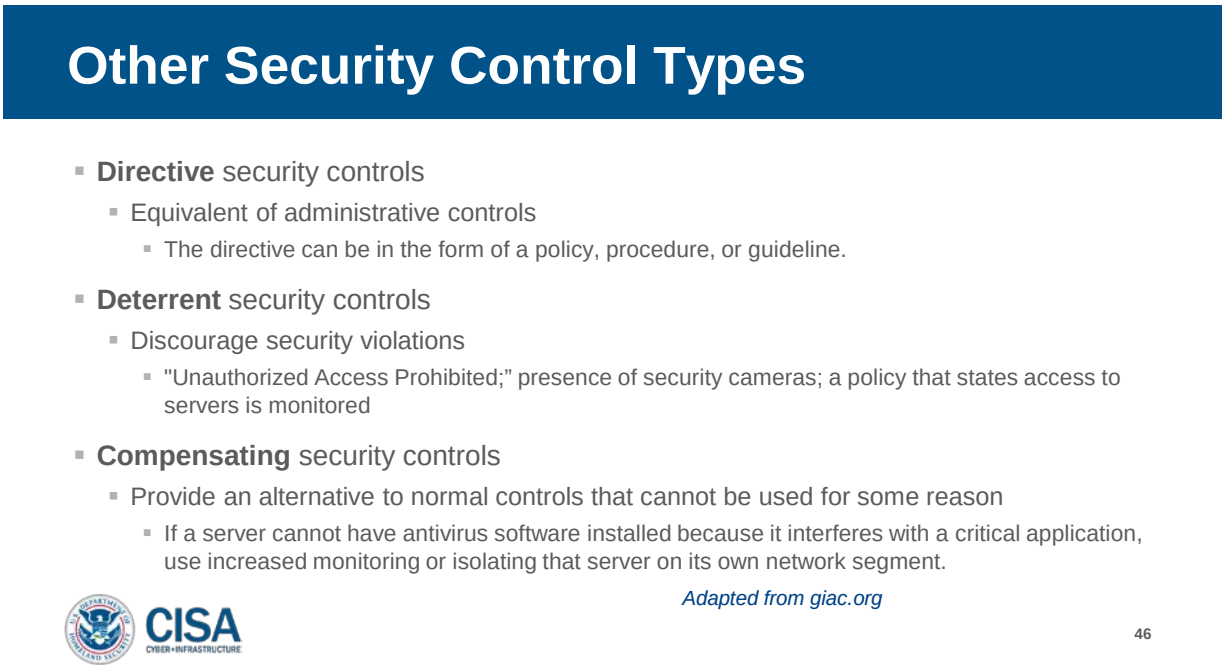
# Recovery Security Controls

- Put a **system back into production** after an incident
- Most **Disaster Recovery** activities fall into this category.
  - After a disk failure, data is restored from a backup tape.
  - Procedures should guide this process.


CISA
CYBER+INFRASTRUCTURE

45

**045 We could also have recovery controls. What we're trying to do here is we're trying to actually get the system back up online to its original productive state. So what we really want to do is we want to understand, for example, how we could recover a disk after it's failed. What are we going to do about restoring that data? Do we have procedures for people to restore that data?

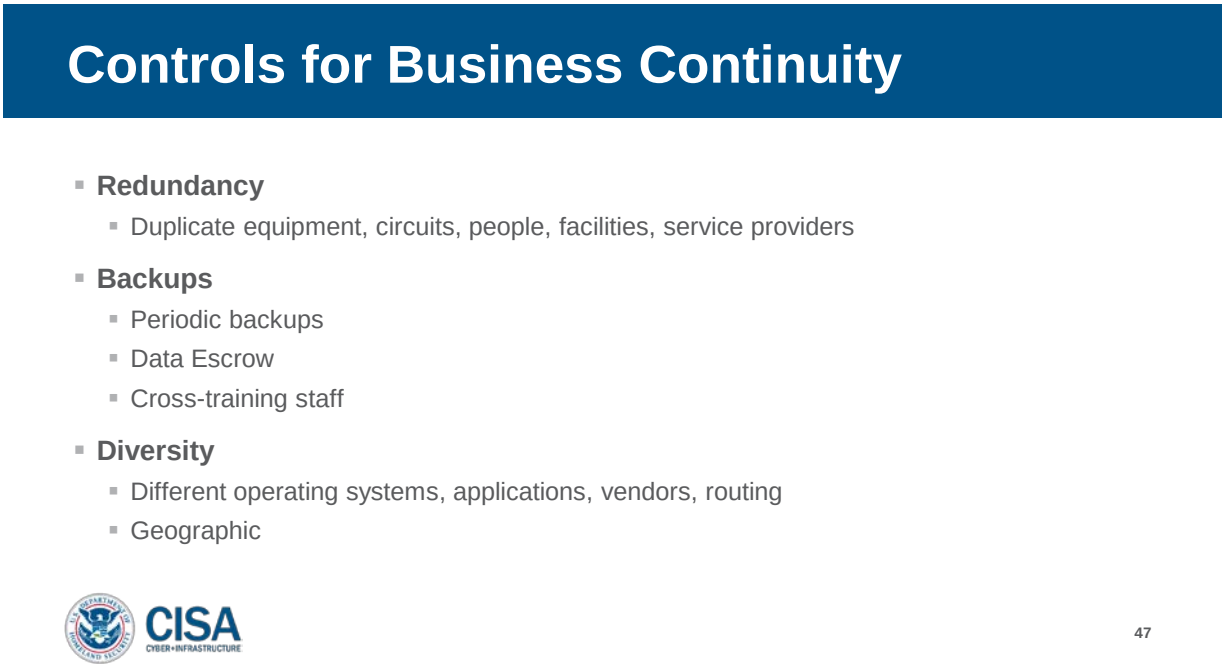



**046 Some other types could be some directive security controls such as administrative controls. These are additional policies or procedures that tell people what specifically they can do. We can actually have deterrent controls. Now this would just deter people from doing bad things. A good example here was the security camera notion where we actually have a security camera up in an organization, and it may not even be one that's being used, but the fact that somebody can see it, it's going to discourage them from doing anything negative.

We could have compensating security controls. Now this is-- say that we have normal controls in place, but for some reason we need additional or some kind of alternative control that would help us. So suppose that we

have antivirus software on our system and it's actually interfering with critical operations that we have. So maybe what we do is we have to isolate that server and we have to have our own network segment. This may be an action that we're taking as a compensating security control.

### Controls for Business Continuity




**047 So we can also have controls that support business continuity. Now remember business continuity is what we want to keep our organization moving despite that risk coming to fruition. A good example here could be we could have redundancy in our system. Maybe we have a critical asset and if we lose it our organization can't operate. So it would be a good idea to have another one in place.

The same idea could be said here for people. Suppose I have a person who knows some critical information, or maybe has a critical skill or capability. I could train another person to have that same skill or capability so that way if that person happens to be sick on any given day, we can turn to this other person that we've trained.

We could also think about backups. Where are we going to store this information if I lose availability of the information that I need to make my enterprise operate? Maybe I give it to another organization to hold in escrow. Another thing I could do here in terms of backups is once again cross-training staff. Now that's that capability idea, but this for backups is thinking more in terms of maybe a person knows something specifically and we're going to actually have the other person know the same thing, so that way if I lose one individual I'll still have access with another individual to execute the same task.

I may also want to think about diversity here. Now what I'm talking about is I have separate systems, and maybe they're doing the same thing, but they may be located in a different place, or maybe they have different applications that do the same thing, maybe made by different vendors altogether. Also I may want to think about geographic diversity. Maybe I have critical assets in one place and I have a mirrored set in yet another place so that way if I lose

one, I have the other set that I can turn to.

## Spare Equipment and Contingency Services

### Spare Equipment and Contingency Services

- Thinking about renting laptops for recovery?
  - Use care in selecting a provider.
  - Understand provider's "policies".
  - Do you have exclusive use?
  - Test the product.
  - Where are they stored?
  - How do you get them in an emergency?
  - Other challenges…

Always vigilant – even during a recovery.

**Laptop Spying: Rental Company Sued Over Alleged Webcam Spying**

*By KI MAE HEUSSNER*

May 4, 2011— go.com

A furniture and electronics rental company accused of using rented laptops to spy on customers in their own homes has already been hit with a lawsuit, and a computer privacy expert said he wouldn't be surprised if the allegations now catch the FBI's attention.

A Wyoming couple on Tuesday filed a lawsuit seeking class action status with a district court in Pennsylvania, citing the Federal Wiretap Act and alleging that Aaron's Inc., an Atlanta-based national rent-to-own chain, secretly spied on them with a laptop rented from a local franchise.

In the suit, Brian and Crystal Byrd claim that, without their knowledge, a computer rented from Aaron's was equipped with software capable of intercepting electronic messages, taking webcam pictures and tracking keystrokes.

The Byrds said they only learned about the spyware when the store manager, incorrectly believing that the couple was in default on their agreement, stopped by their house in December 2010 with a picture of Brian Byrd taken remotely with the computer's webcam.

Several legal experts told ABC News that although the rental company may have the right to use technology to track their property or shut it down if customers don't pay, the customers need to be told when they are being monitored.

"It's really, really outrageous behavior," said Paul Ohm, an assistant professor at the University of Colorado Law School. "To me, this seems to cross all sorts of ethics lines and lines of custom."

http://abcnews.go.com/Technology/laptop-spying-rental-company-sued-alleged-webcam-spying/story?id=13528292

CISA CYBER+INFRASTRUCTURE

48

**048 What we have here is we have spare equipment and contingency services. The way we think about this is suppose I have an organization that is looking at a risk that could come to fruition where I need additional laptops, and I can actually go to them and rent twelve laptops at the drop of a hat if that risk were to come to fruition, but what I need to do before I go and do this is think about what provider I'm selecting and how I'm going to do it, what policies I'm going to have in place to control what this provider has in terms of information and assets that my organization is going to give them, because they're going to give it back when I need at that bad day.

Do I have exclusive use of those computers? Think about this: If there's an organization that is resident in a city and a tornado hits that city and I lose the computer and laptops that I need, call up the individual and say, "Hey, I need those laptops now," and he's like, "Hey, sorry to say, but I've already given it to two other clients that had the same exact contract with me." You want to make sure that you have exclusive access to those assets that you have licensed for and that you're paying for.

You may also want to test the product, because it's going to sit in a service locker somewhere. You want to make sure that at a moment's notice you can open it up, turn it on, and you can get your organization back up and running in no time. Think about where they're stored. If that service locker is in the same city where that tornado is going to hit, this could be a problem because that same locker that has your backup computers could be swept away. You really want to think about too how are you going to truly get to them in an emergency. You always want to be vigilant.

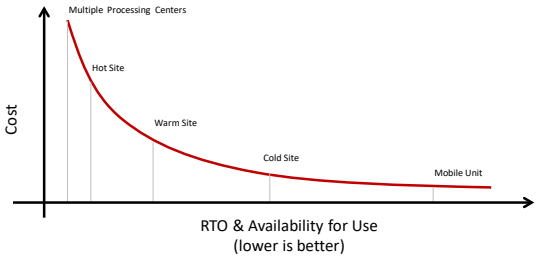
A good example here too is you want to think about the provider and you want to vet them well. In this particular case where I have an example here, you actually had a laptop service that was providing the same rental idea, but they were salvaging or taking or stealing information off those computers and

using it for their own nefarious reasons.

### Alternate Storage and Processing Sites

## Alternate Storage and Processing Sites

- A number of different strategies exist.
  - The right one will **depend on the business needs**.
    - Recovery Point Objective, Recovery Time Objective, cost, availability, capabilities, speed, access, etc.
- Make sure to consider
  - Physical security, staffing, utilities (water/power), environment




CISA CYBER+INFRASTRUCTURE

49

**049 Now, let's talk about that diversity in geographic location here. You want to think about this in terms of having maybe alternate storage and processing sites. There's a lot of different strategies that exist right here that we could talk about, but remember we want to keep in mind at what point do I lose so much data that I can no longer keep my organization operating? That's my recovery point objective. I may also have a period of time that I have to think about where, if I'm not recovered, my organization is not going to be able to get back up to its original state.

And by the way, this all costs money, so we want to think about what we're

going to do in terms of what we're willing to pay for to suit our risk appetite.

So you want to think about a lot of different things here. You want to think about physical security of those sites. Am I going to staff both those sites? Maybe a site is remote and it's largely operated by just a ghost staff, or maybe a skeleton crew of maybe one to two people. What kind of utilities are necessary and will they always be available? What kind of environment is it? Can I trust it?

## Notices