Considerations for Responding to Risks

Table of Contents

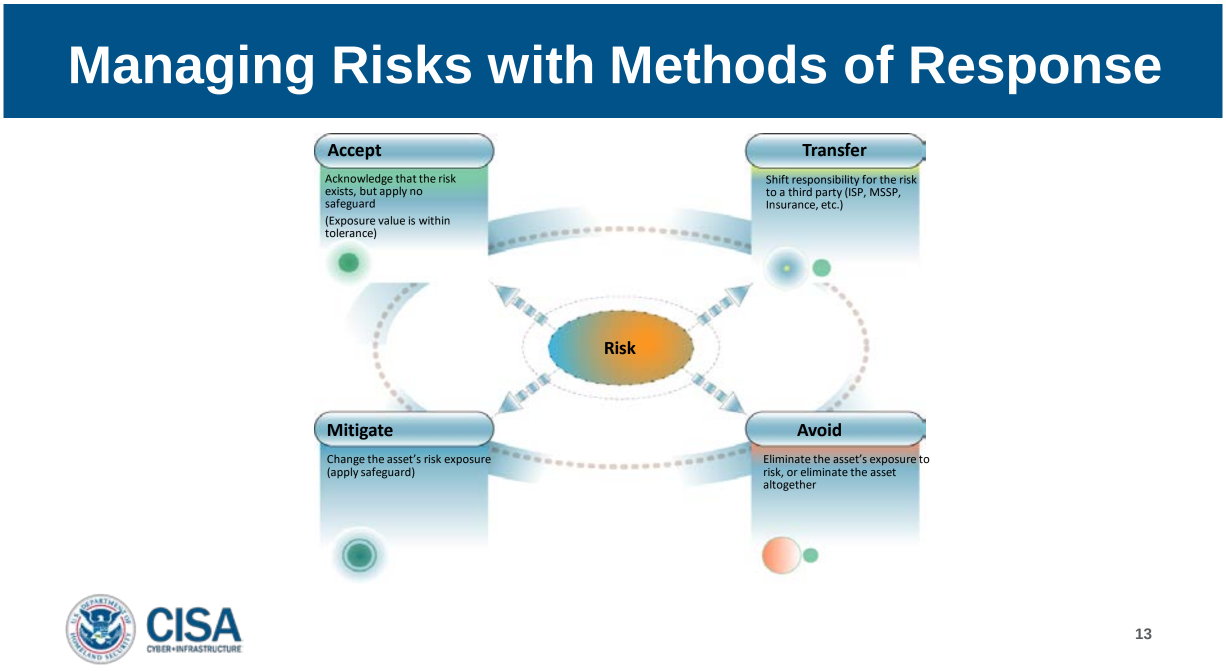
Risk and Impact Analysis

Risk and Impact Analysis

12

**012 Instructor: And right now we're going to talk about risk and impact analysis and we make consideration for responding to risks.

Managing Risks with Methods of Response



Managing Risks with Methods of Response

Accept

Acknowledge that the risk exists, but apply no safeguard

(Exposure value is within tolerance)

Transfer

Shift responsibility for the risk to a third party (ISP, MSSP, Insurance, etc.)

Risk

Mitigate

Change the asset's risk exposure (apply safeguard)

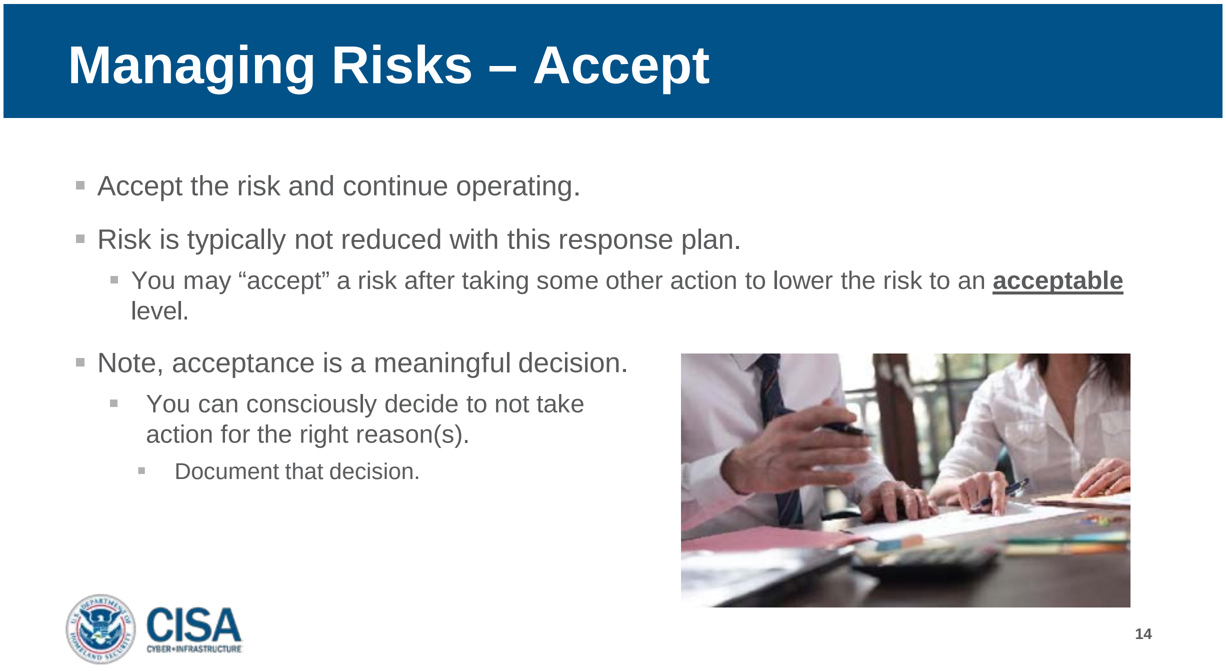
Avoid

Eliminate the asset's exposure to risk, or eliminate the asset altogether

13

**013 We can manage risks by thinking about how we're going to actually respond to them. You can do this in any variety of ways, but there are four main strategies that you want to think about. You can accept a risk, you can transfer it, you can avoid it, or you can mitigate it. So let's look a little bit closely at these strategies and see a little bit more about what they're all about.

Managing Risks – Accept



Managing Risks – Accept

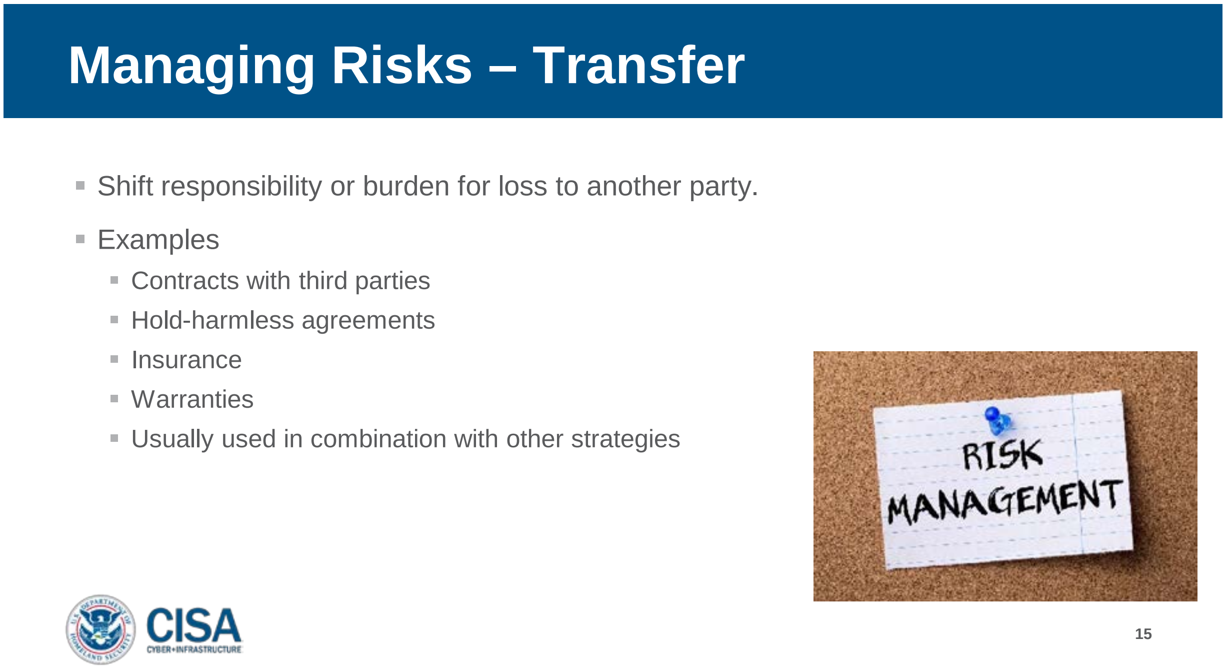
- Accept the risk and continue operating.
- Risk is typically not reduced with this response plan.
  - You may “accept” a risk after taking some other action to lower the risk to an **acceptable** level.
- Note, acceptance is a meaningful decision.
  - You can consciously decide to not take action for the right reason(s).
    - Document that decision.

CISA
CYBER+INFRASTRUCTURE
14

**014 One of our strategies is we can actually accept the risk. This means that we're going to just operate with the risk existing, and we're really not going to do anything to invest resources to manage it or bring the likelihood to an acceptable level, really. That said, understanding that we have an appetite in the organization, we're going to just let the risk happen if it happens. And by the way, this is not just feeling lazy about it and just letting the risk happen; technically this is a meaningful decision. What you want to do is document it and make sure that you've accepted this risk based upon all the information that you have available. And you also want to understand that you're saving yourself resources to address other risks. You're not just going to go out and spend that money like it's fun money.

So acceptance is actually a very critical decision. Some risks you may just accept because they have a lower impact or a lower likelihood, and that's fine, but make sure it's a meaningful decision.

Managing Risks – Transfer



Managing Risks – Transfer

- Shift responsibility or burden for loss to another party.
- Examples
  - Contracts with third parties
  - Hold-harmless agreements
  - Insurance
  - Warranties
  - Usually used in combination with other strategies

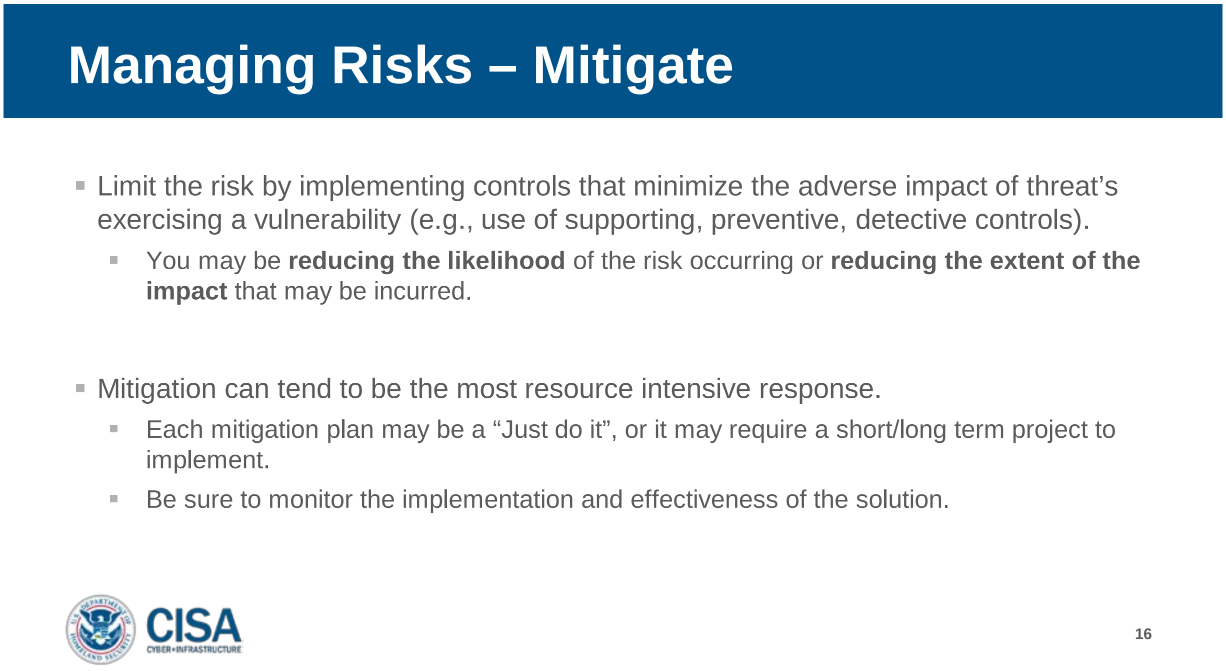
RISK
MANAGEMENT
CISA
CYBER+INFRASTRUCTURE

15

**015 Otherwise, I may want to partner with other organizations to share the burden of this risk. Classically we may think about this example in terms of insurance. You may buy insurance and transfer that risk to that insurance carrier, and you're paying them for their troubles, but to be honest, if the risk were ever to come to fruition, they would actually have to pay into recovery from that risk coming to fruition.

You can think about this other ways too. We can establish contracts with third-parties, other vendors. We can actually have some agreements in place to say that a certain partner is willing to take on a certain amount of risk. We can have warranties for our products. You can also combine these together.

Managing Risks – Mitigate



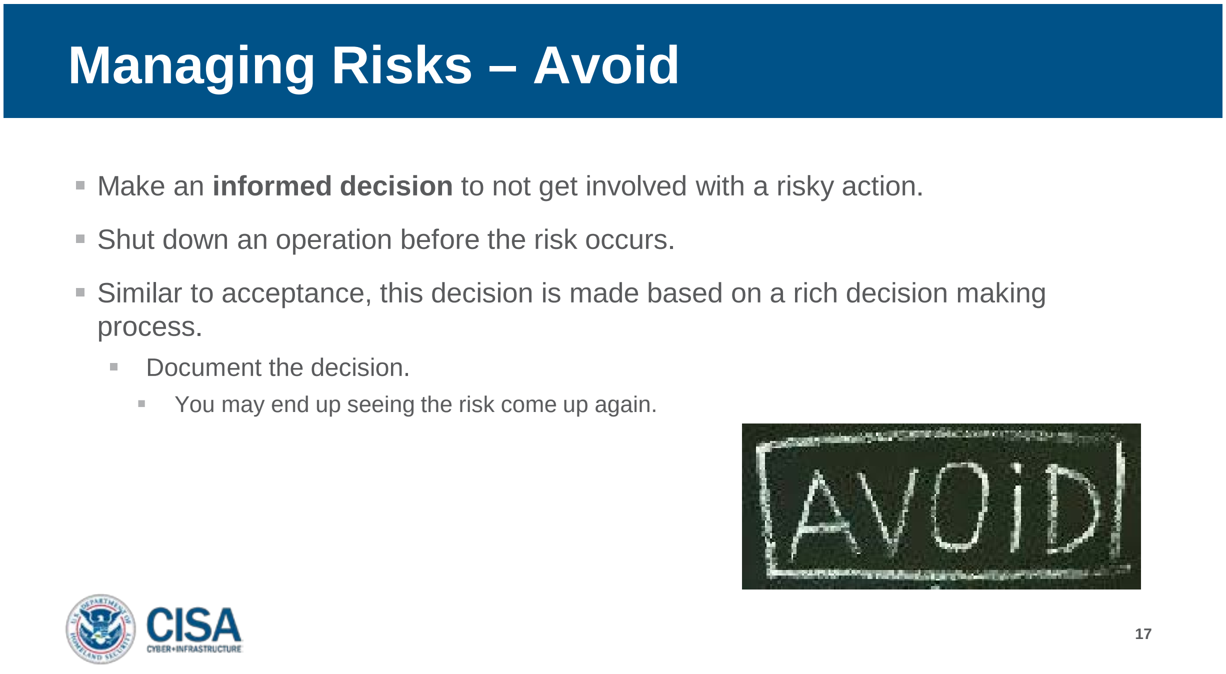
Managing Risks – Mitigate

- Limit the risk by implementing controls that minimize the adverse impact of threat’s exercising a vulnerability (e.g., use of supporting, preventive, detective controls).
  - You may be **reducing the likelihood** of the risk occurring or **reducing the extent of the impact** that may be incurred.
- Mitigation can tend to be the most resource intensive response.
  - Each mitigation plan may be a “Just do it”, or it may require a short/long term project to implement.
  - Be sure to monitor the implementation and effectiveness of the solution.

**016 We can also think about taking action, and this is called mitigation of a risk, and what we really want to do is we want to invest resources wisely such that we either reduce the likelihood of the risk or we reduce the amount of pain or impact that you would feel if the risk were to come to fruition. This is really the cool trick about risk management. You could actually have, in a sense, a crystal ball in your risk assessment, looking ahead to the future and understanding what I could do to keep that risk from ever happening. But when that cold, dark day comes, you could also understand that you have resources standing by to recover from that disaster and keep your business operating.

So what you want to do is you want to set up a plan. Sure you may have some items that are "just do its", if you will. But if you have some controls and/or response plans that are going to take longer than just a few days or maybe even considerable resources that are necessary for investment, be sure to set up a project plan of some sort so that way you can mindfully implement that control, and it's done in a way that you can monitor its implementation and effectiveness.

Managing Risks – Avoid



Managing Risks – Avoid

- Make an **informed decision** to not get involved with a risky action.
- Shut down an operation before the risk occurs.
- Similar to acceptance, this decision is made based on a rich decision making process.
  - Document the decision.
    - You may end up seeing the risk come up again.

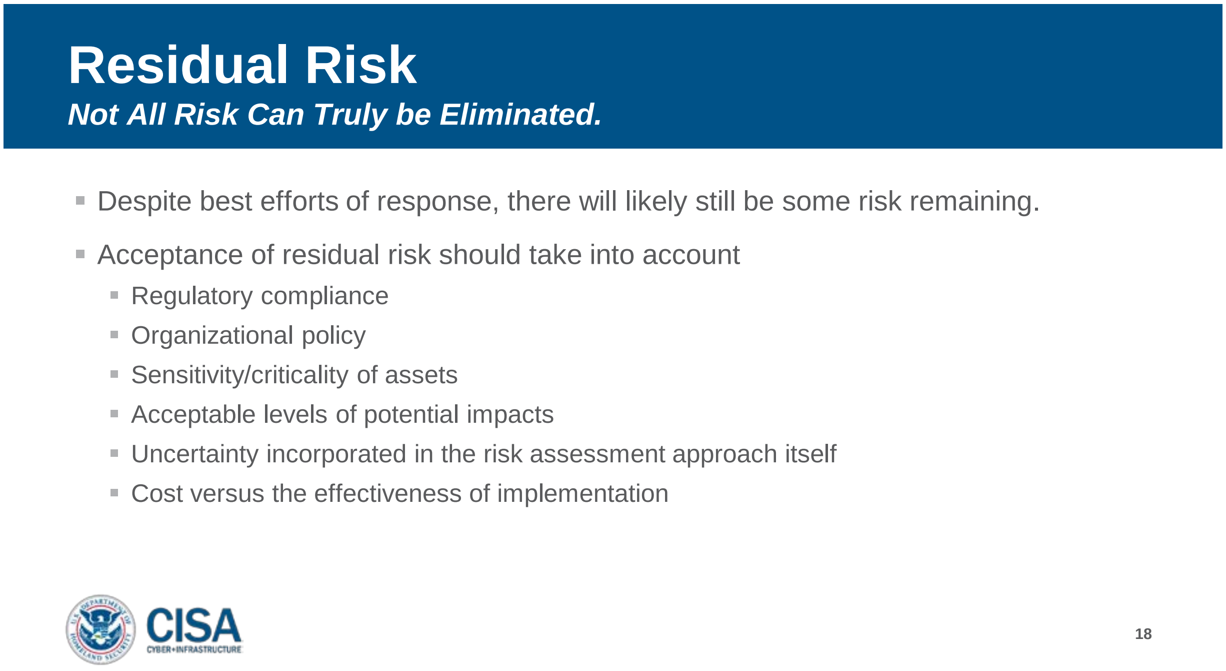
AVOID
CISA
CYBER+INFRASTRUCTURE

17

**017 You also could go about avoiding a risk altogether, and this is another informed decision. Similar to acceptance, but to be honest with you, you're not going to engage in the activity at all. With acceptance, you may have still stayed with the mission, but on this one, you're avoiding it altogether. And you got to think about this in a very meaningful way too, because there may be an opportunity cost that you're losing there as well.

So you want to think about this in terms of acceptance as well, but you're also very much documenting this decision. You're making a mindful decision, and you want to know why. Especially down the road, if something were to change and people started asking why you made the decision, you'll have it documented.

Residual Risk Not All Risk Can Truly be Eliminated.



Residual Risk

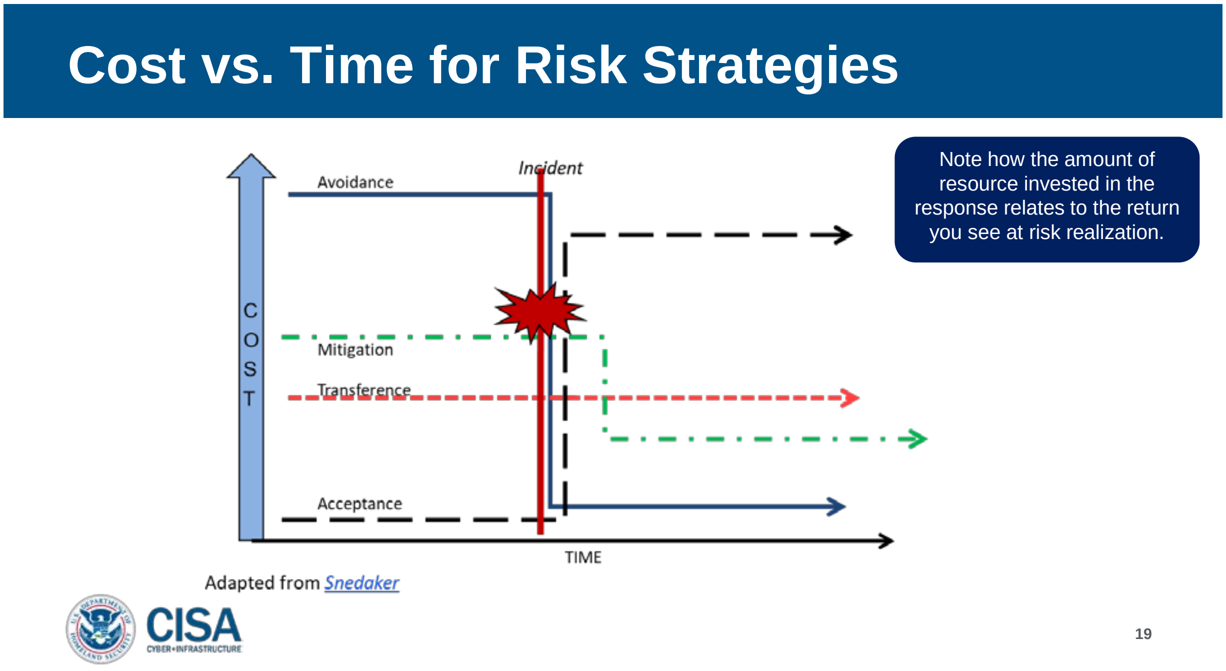
Not All Risk Can Truly be Eliminated.

- Despite best efforts of response, there will likely still be some risk remaining.
- Acceptance of residual risk should take into account
  - Regulatory compliance
  - Organizational policy
  - Sensitivity/criticality of assets
  - Acceptable levels of potential impacts
  - Uncertainty incorporated in the risk assessment approach itself
  - Cost versus the effectiveness of implementation

**018 So remember, no matter what controls you put into place, not all risk can truly be eliminated. So no matter what you do, you may still have some uncertainty left on the table, if you will, and you're going to have to look through different lenses to understand if you've really met the appetite of the organization. You've got to be careful if there's some sort of regulatory compliance matter that you have to follow up, so that way you have to knowingly dial your risk down to a certain level.

For example, it is unacceptable to release HIPAA data to the public. If that's the case, you have to go to great extremes to make sure that that residual risk is to an absolute minimum to the best of your capability, and that's going to be a regulatory issue. It may be an organizational policy. Maybe you have some assets that have some certain amount of sensitivity to it, where you have lower levels of information that may be okay and have minimal impact to the organization if it's released, but if it is a data set or an information set that has high sensitivity levels, maybe it's top secret to your organization, that could be driving your decision as to whether or not you need to invest more resources to insulate those particular assets. So you want to think about the cost of what you're investing around the security and the controls that you're putting into these risks to address them, versus what you're going to get on the other side, effectively like a return on investment for what you're-- in this case, it's a return on risk investment.

Cost vs. Time for Risk Strategies



Cost vs. Time for Risk Strategies

Note how the amount of resource invested in the response relates to the return you see at risk realization.

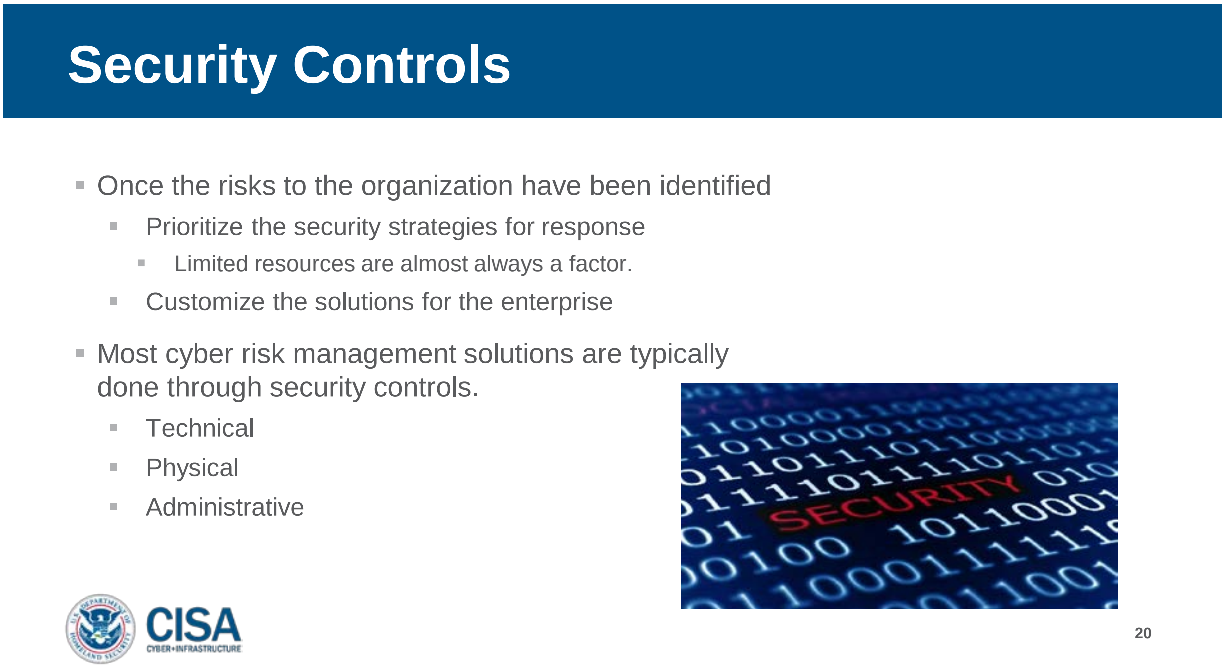
Adapted from *Snedaker*

19

**019 You can think of this in different ways. We've talked about the avoidance, mitigation, transference and acceptance strategies, and what you really want to do is put yourself in the seat of that cold, dark day again when that risk comes to light. If you've avoided the risk altogether and the incident happens, there may have been a really high cost related to that avoidance because, let's face it, you didn't go down the path to make that revenue, so it was a lost opportunity. But if an incident happens, you really have no loss, so there may be a good balance that's struck there.

Same thing to be said with mitigation, where you may have an investment of resources to dial a risk down, and you're hoping that past the incident, you've at least brought down the cost related to that risk coming to fruition.

Security Controls



Security Controls

- Once the risks to the organization have been identified
  - Prioritize the security strategies for response
    - Limited resources are almost always a factor.
  - Customize the solutions for the enterprise
- Most cyber risk management solutions are typically done through security controls.
  - Technical
  - Physical
  - Administrative

SECURITY
CISA
CYBER+INFRASTRUCTURE

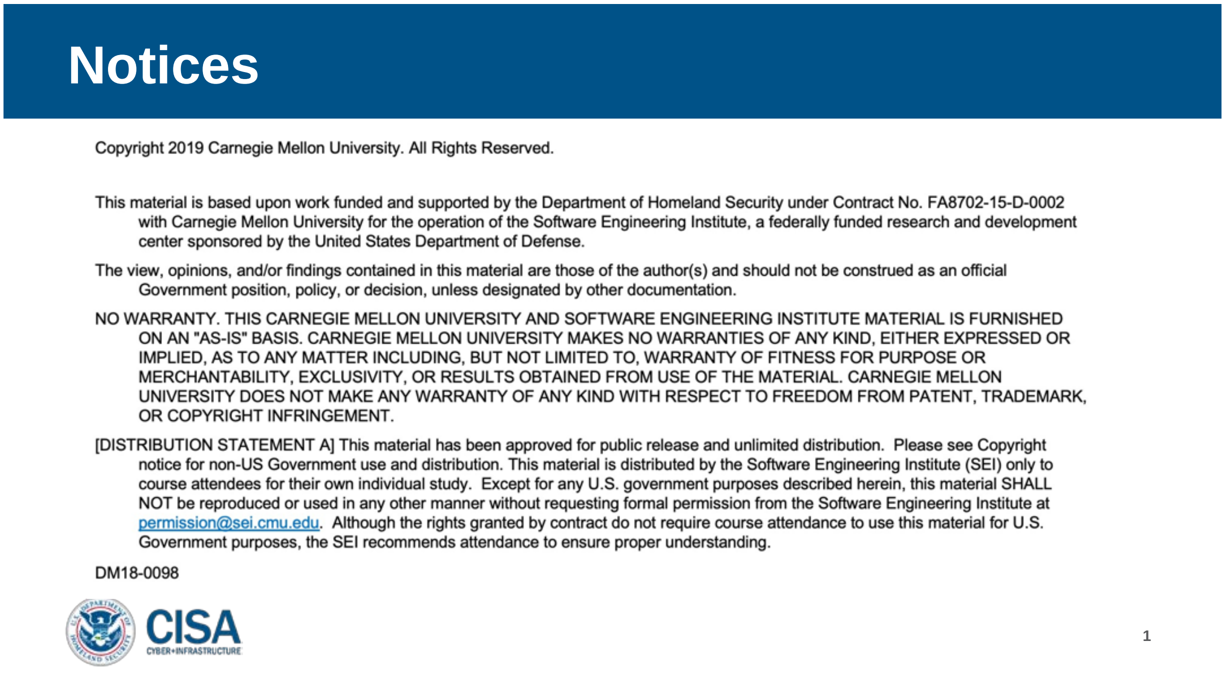
20

**020 So now that you have your strategy in place as to how you're going to address that risk, let's talk a little bit about how you're actually implement the controls around it.

So first thing you want to do, you've identified these risks. You really want to prioritize the strategies that you've put into place for a response, and recognizing that you have only a certain number of resources that could be actually put to this risk management game, you want to understand where I'm going to get the biggest return on my risk investment, and in some cases you may want to consider how you're going to actually customize these solutions such that you get that maximization of your resources. Remember, there's a critical win here for risk managers in finding the interdependency of risks and how they're related. Maybe a response for one risk will help you with multiple other risks. That may bring a risk response to a higher level of prioritization because you can get more return on your risk investment in that case.

When we do this, we want to do it using security controls through three basic avenues. They could be technical controls, they could be physical controls, or they could be administrative.

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