Vulnerabilities

Table of Contents

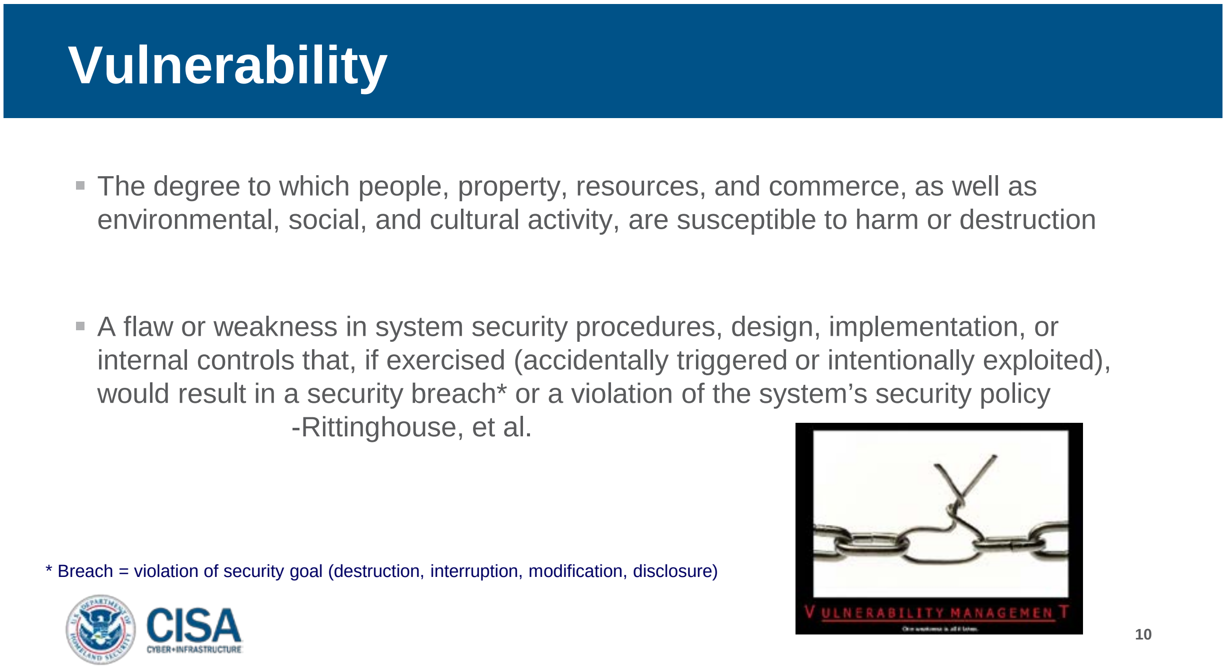
Vulnerabilities

Vulnerabilities

9

**009 Instructor: I'm here to talk to you today about vulnerabilities. So what is a vulnerability?

Vulnerability



Vulnerability

- The degree to which people, property, resources, and commerce, as well as environmental, social, and cultural activity, are susceptible to harm or destruction

- A flaw or weakness in system security procedures, design, implementation, or internal controls that, if exercised (accidentally triggered or intentionally exploited), would result in a security breach* or a violation of the system's security policy
  -Rittinghouse, et al.

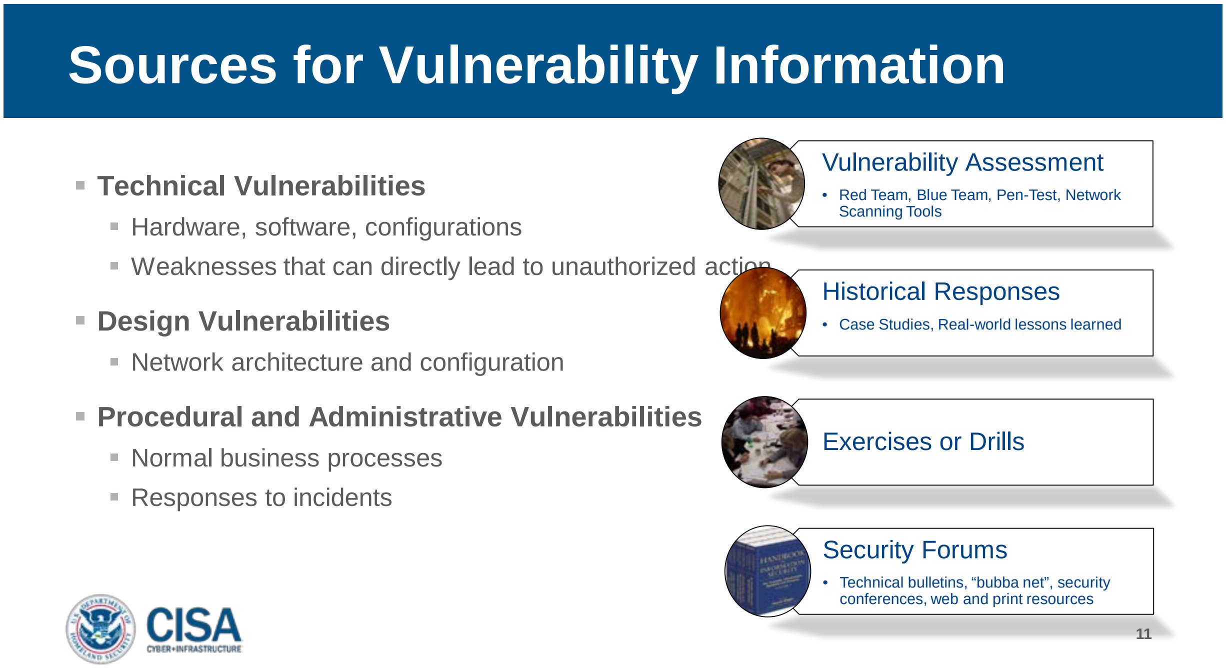
* Breach = violation of security goal (destruction, interruption, modification, disclosure)

CISA
CYBER+INFRASTRUCTURE

10

**010 Well, simply put, it's the degree to which our fundamental assets might have some kind of weakness, some kind of gap that allows harm to enter into my system, that may actually bring my enterprise to its knees, if you will. So we think about this as like a flaw, if you will. Now, by the way, it may be an intentional flaw, or it may be a mistake in the system, but in all cases, it's that weak link.

Sources for Vulnerability Information



Sources for Vulnerability Information

- Technical Vulnerabilities
  - Hardware, software, configurations
  - Weaknesses that can directly lead to unauthorized action
- Design Vulnerabilities
  - Network architecture and configuration
- Procedural and Administrative Vulnerabilities
  - Normal business processes
  - Responses to incidents

Vulnerability Assessment
- Red Team, Blue Team, Pen-Test, Network Scanning Tools

Historical Responses
- Case Studies, Real-world lessons learned

Exercises or Drills

Security Forums
- Technical bulletins, “bubba net”, security conferences, web and print resources

CISA CYBER+INFRASTRUCTURE

11

**011 There are many different sources for vulnerability. We may think about it in terms of technical vulnerabilities. So maybe I have flaws in my hardware, or classically, in software, where I'll have maybe something that is programmed into the system, a backdoor, for example, where threat actors can get in, penetrate the system, and do things that are not necessarily going to result in a positive outcome for me.

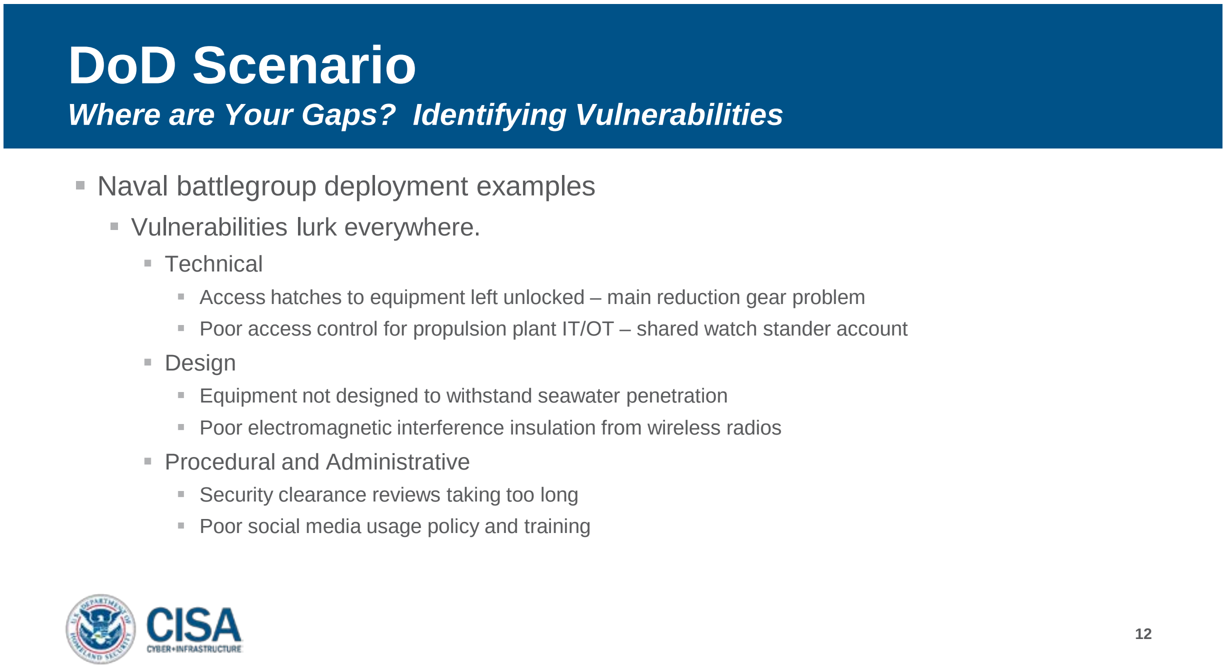
Maybe I have witnesses that lead to unauthorized action. So let's go back to the backdoor idea. I can actually let people in, whether an insider or an external actor that maybe could get into the system, and they can actually create some pretty adverse impacts for me. This comes down to maybe even a design vulnerability.

Maybe, for example, I don't have proper configuration for my network.

You could also think about this in terms of procedures and the things that people do. If the procedure's not written correctly and someone were to, let's say, do something that is per the procedure but the way it's written is incorrect, and actually have a flaw in the system, I could really bring my enterprise down a notch in terms of being fully operational. I could really have some damage, some negative outcome that takes place there, and how would I go about identifying these? I can do vulnerability assessments. You know, we have red teaming, we have penetration testing, and we have a variety of network scanning tools that exist that you could go find these vulnerabilities. By the way, make sure that those network scanning tools are staying up to date.

We could also look back at historical responses. So we could look back at organizations similar to ours, benchmark, if you will, and look at case studies or look at, like, real-world lessons learned that we have related to the organization and see what took place before. We could also do a real-time exercise or run a drill to see how people respond in a pressure situation. That could identify vulnerabilities in training, and we could also talk to others in our community. We could have, like, a security forum, if you will. Some people call this a bubba net, but basically, it's calling up somebody you know in the industry and ask them what they think about an issue, if they've seen something similar.

DoD Scenario Where are Your Gaps? Identifying Vulnerabilities



DoD Scenario

Where are Your Gaps? Identifying Vulnerabilities

- Naval battlegroup deployment examples
  - Vulnerabilities lurk everywhere.
    - Technical
      - Access hatches to equipment left unlocked – main reduction gear problem
      - Poor access control for propulsion plant IT/OT – shared watch stander account
    - Design
      - Equipment not designed to withstand seawater penetration
      - Poor electromagnetic interference insulation from wireless radios
    - Procedural and Administrative
      - Security clearance reviews taking too long
      - Poor social media usage policy and training

CISA
CYBER+INFRASTRUCTURE

12

**012 So imagine we're a Navy battlegroup and we're deploying and we're going to sea, and we're going to maybe a region that is somewhat in turmoil. So if you think about it we have large capital assets. We have maybe a carrier, a cruiser, destroyers, submarines, air assets. We have a lot of equipment and material and vital critical assets that are going over the horizon. We want to think very carefully about the vulnerabilities that may be lurking within that battlegroup, and let's break it down.

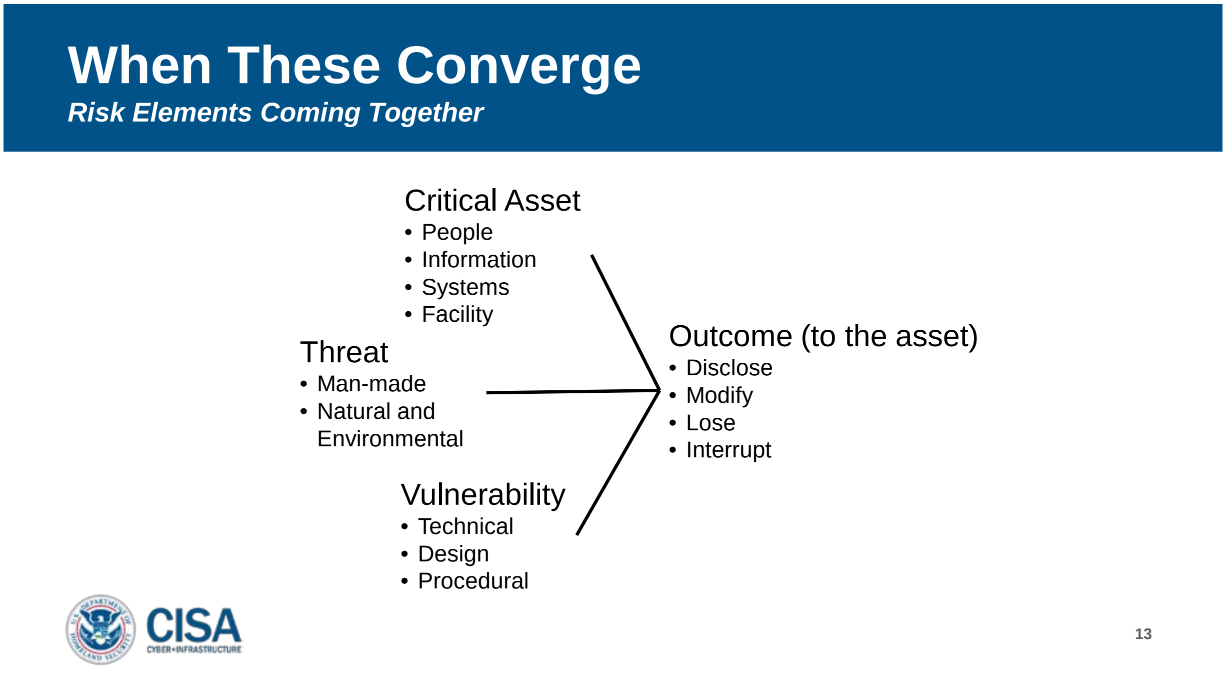
Like I said, we could have technical vulnerabilities, and this could be something simple as access hatches to equipment that are left unlocked. You know, I think back to my time in the Navy and I actually think about how the chief engineer was the only one who had keys that could access the main reduction gear. Well, clearly, the main reduction gear is something that drives the ship. The engines would actually propel the gear that actually propels the propeller, and if I were to destroy that main reduction gear, I'm dead in the water. So the chief engineer kept the key so that way you don't have some disgruntled sailor that opens it up and throws a bucket of sand in your main reduction gear.

You may also think about this in terms of an IT/OT kind of a thing, where you think about the propulsion plant and you may have a disgruntled sailor, once again, or maybe even a threat actor. Suppose you have, let's say, a ship repair worker who comes on the ship and they are an inside threat actor that could actually negatively impact your control systems in your reactor plant or your engineering plant, excuse me.

Could be a design issue. Suppose I have some equipment that is on the weather decks. Maybe a weapons system or something like that, and it wasn't properly sealed and allowed seawater in and it destroys the electronics. Maybe it's an EMI or electromagnetic interference issue, where if I bring, have personnel that bring wireless radios on board the ship, maybe even for good reasons, suppose they're using it for damage control operations or things like that, and that EMI interferes with existing equipment and shuts it down.

I could also have procedural or administrative challenges. So think about this. If I have, let's say, a security clearance review process where I have granted internal clearance but it takes too long and I miss somebody who wouldn't actually necessarily come up as maybe not being qualified to have a certain security clearance or level. So there's a gap there. I want to think about how I would address and correct that situation so that way I have the proper controls up.

When These Converge Risk Elements Coming Together



When These Converge

Risk Elements Coming Together

Critical Asset
- People
- Information
- Systems
- Facility

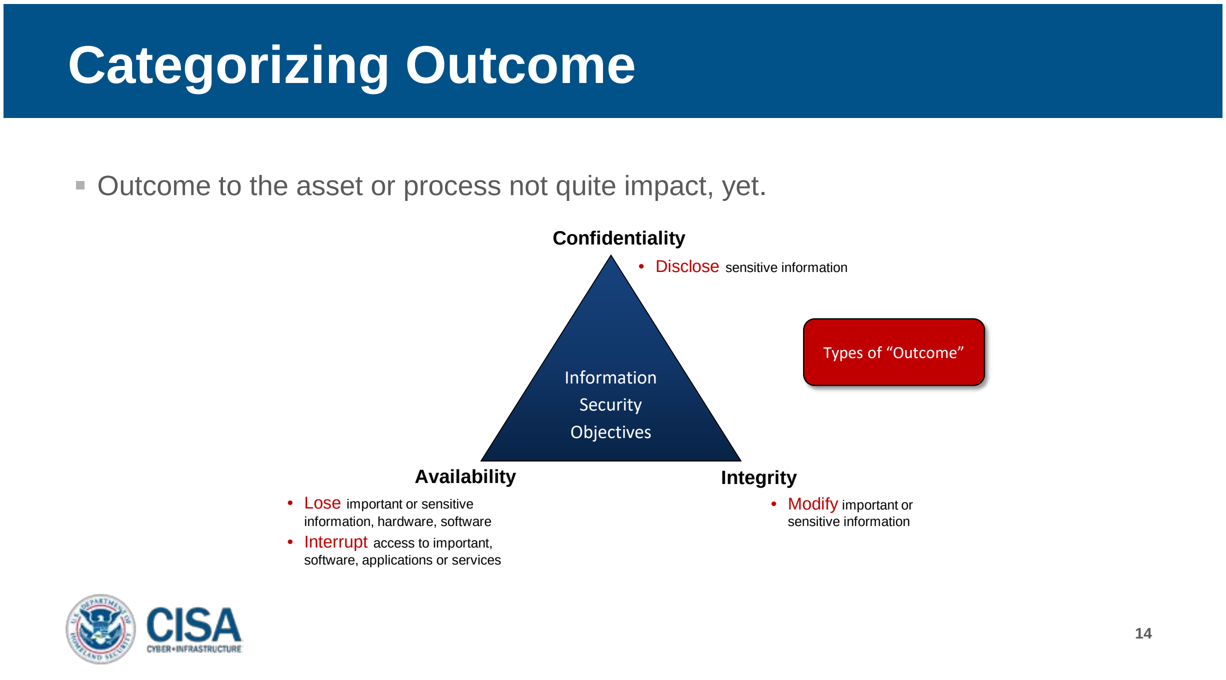
Threat
- Man-made
- Natural and Environmental

Vulnerability
- Technical
- Design
- Procedural

Outcome (to the asset)
- Disclose
- Modify
- Lose
- Interrupt

**013 So we've talked about critical assets. We've talked about the things that are threats to those assets. We've talked about the vulnerabilities. So really what it's coming down to is we have all these elements lined up that could actually come together and create and outcome for our organization. Remember, when we think about outcomes, we want to think about things in terms of information being confidential, having integrity for that information, and having it be available to the enterprise.

Categorizing Outcome



Categorizing Outcome

- Outcome to the asset or process not quite impact, yet.

Confidentiality

- Disclose sensitive information

Information Security Objectives

Types of "Outcome"

Availability

- Lose important or sensitive information, hardware, software
- Interrupt access to important, software, applications or services

Integrity

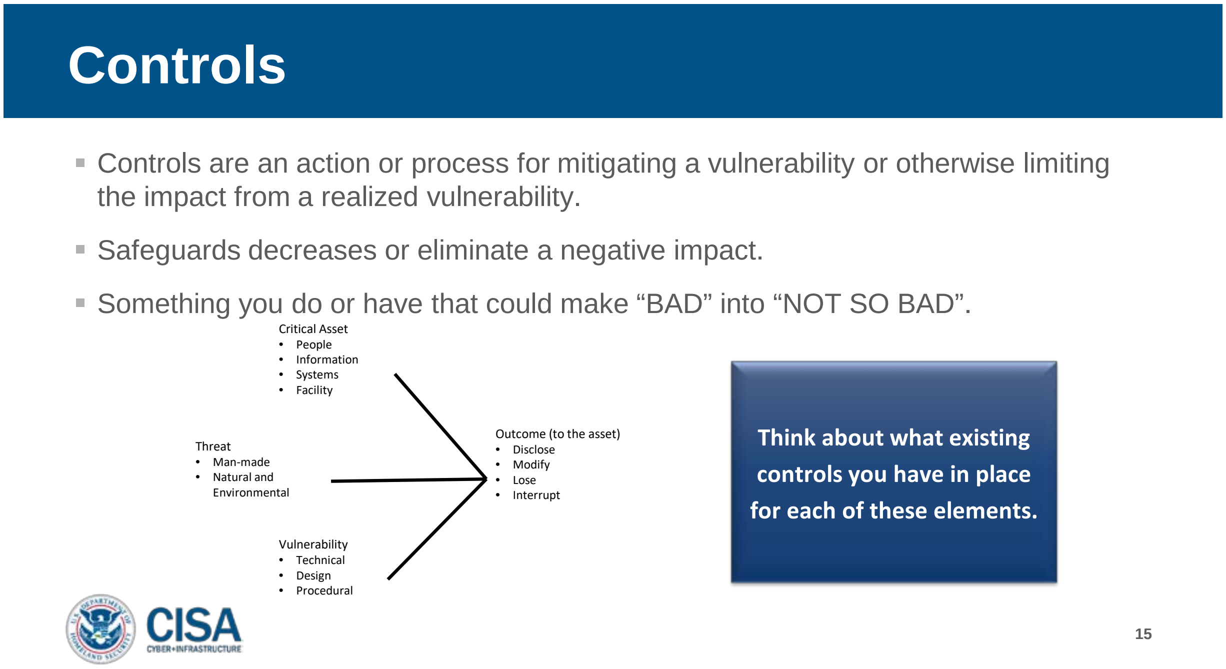
- Modify important or sensitive information

CISA CYBER+INFRASTRUCTURE

14

**014 This can be easily summarized by looking at this graphic here, and you want to think about, "Hey, in confidentiality space, what would disclosure really do to my organization?" In terms of integrity, if I have data and it should become corrupted, how would that impact my enterprise negatively? How about availability? Let's think about if I were to lose pieces or access to certain systems. How would I come dead in the water and how would I recover from something like that?

Controls



Controls

- Controls are an action or process for mitigating a vulnerability or otherwise limiting the impact from a realized vulnerability.
- Safeguards decreases or eliminate a negative impact.
- Something you do or have that could make “BAD” into “NOT SO BAD”.

Critical Asset
- People
- Information
- Systems
- Facility

Threat
- Man-made
- Natural and Environmental

Vulnerability
- Technical
- Design
- Procedural

Outcome (to the asset)
- Disclose
- Modify
- Lose
- Interrupt

Think about what existing controls you have in place for each of these elements.

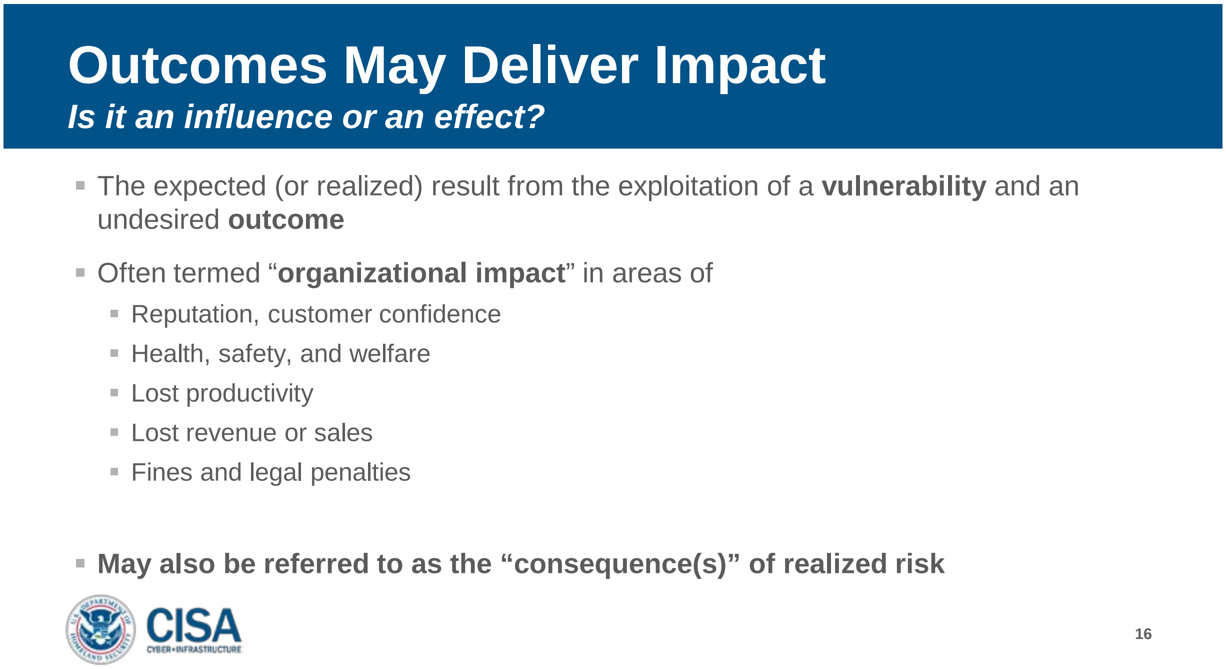
CISA CYBER+INFRASTRUCTURE

15

**015 So in answering that question, what I really want to think about are the controls I want to set up around these assets such that I don't realize these outcomes. You also want to think about the controls that you already have that are resident in the system. I like to use the example of a fire. Because a lot of buildings that you walk through, a lot of facilities, they already have sprinkler systems. They have fire alarms that can be used.

So we want to think about the controls that we already have existing, because we don't want to replicate those with our critical resources when we already have something in place.

Outcomes May Deliver Impact Is it an influence or an effect?



Outcomes May Deliver Impact

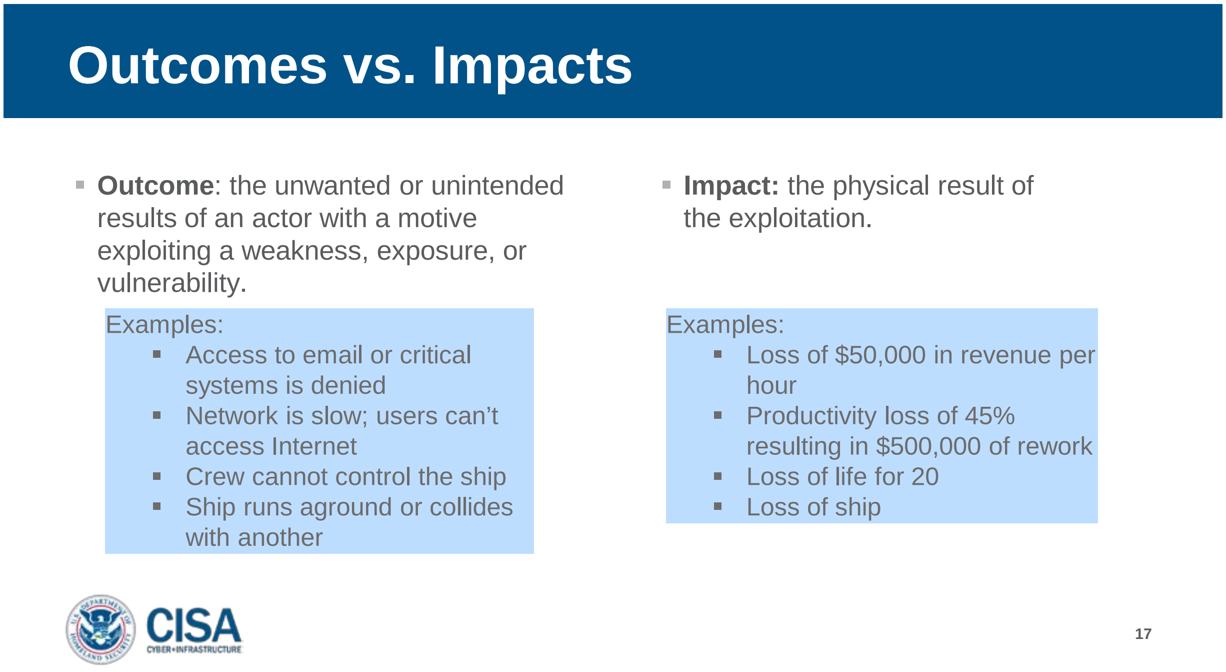
Is it an influence or an effect?

- The expected (or realized) result from the exploitation of a **vulnerability** and an undesired **outcome**
- Often termed "**organizational impact**" in areas of
  - Reputation, customer confidence
  - Health, safety, and welfare
  - Lost productivity
  - Lost revenue or sales
  - Fines and legal penalties
- **May also be referred to as the "consequence(s)" of realized risk**

**016 So we want to think about too these outcomes, it's not just the fact that we have the outcome. We want to think about the impact that the outcome delivers to the organization. An outcome may be something that's a no, never mind. But really, truly what we're looking for are the undesired outcomes, the ones that really hurt or where we feel pain in the organization.

Lost productivity is a classic example here. If I have a manufacturing facility and I lose a critical piece of equipment for whatever reason, maybe it just breaks down, and I'm actually not getting product out the door, I'm losing money. So it translates to the pain of feeling loss on revenue. Maybe it comes out to a fine or legal penalty. Once again, money going out the door. I feel the pain. Unfortunately, maybe it's somebody who gets hurt, or maybe their actual safety is violated. That, once again, I feel pain, because not only have I have physical pain for that poor individual, but also, I am in a state where I've lost a critical asset in that individual supporting my critical service.

Outcomes vs. Impacts



Outcomes vs. Impacts

- **Outcome**: the unwanted or unintended results of an actor with a motive exploiting a weakness, exposure, or vulnerability.

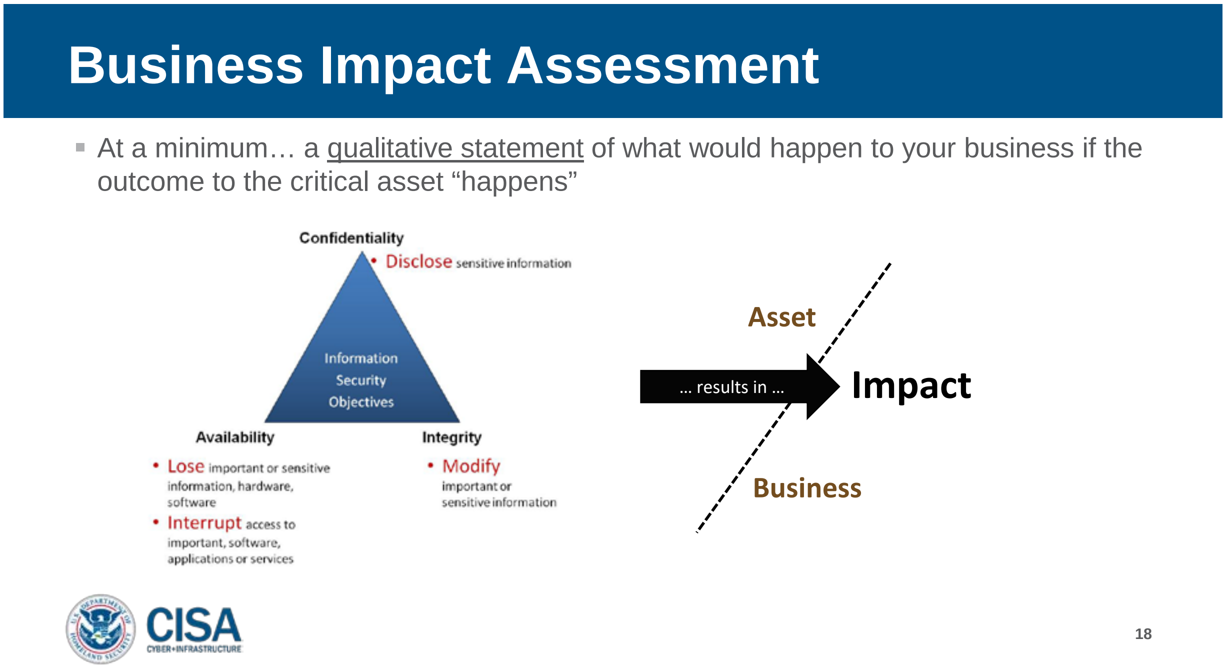
  Examples:
  - Access to email or critical systems is denied
  - Network is slow; users can't access Internet
  - Crew cannot control the ship
  - Ship runs aground or collides with another

- **Impact:** the physical result of the exploitation.

  Examples:
  - Loss of $50,000 in revenue per hour
  - Productivity loss of 45% resulting in $500,000 of rework
  - Loss of life for 20
  - Loss of ship

**017 So let's take this one step further and look at some examples. Some classic examples of outcomes could be maybe some adversarial actor gains access to email or maybe a critical system, or maybe, worse yet, my availability to that system is denied. Maybe the network just bogs down for a time. Maybe it gets slow. Or let's go back to the battlegroup example, where I have maybe a crew that can't control a ship. Maybe they lose control of steering systems, or maybe the ship runs aground. Now, these are all outcomes for risks coming to fruition, but truly, what we have is pain that's felt on the other side in terms of impact. Maybe by getting loss of that system I lose revenue because I am not able to get emails out there or proper marketing materials. Maybe I have a productivity loss. Maybe I've lost life, or maybe I lose a large capital asset like a ship that was going to deliver on a mission.

Business Impact Assessment



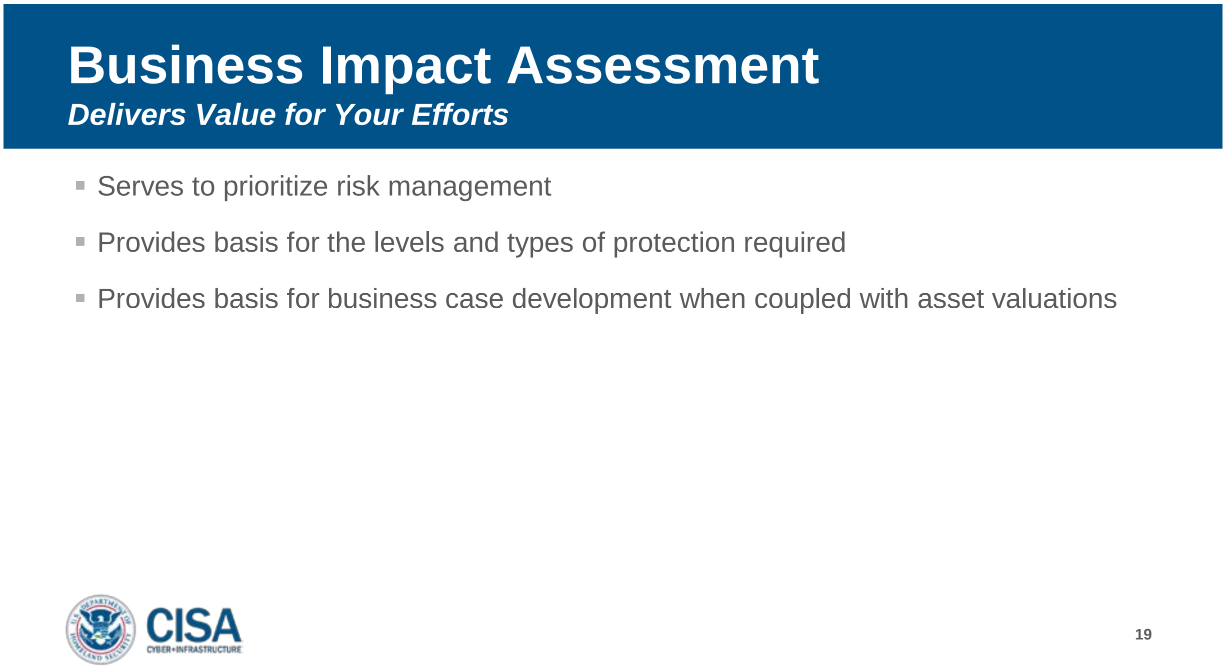
Business Impact Assessment

- At a minimum… a qualitative statement of what would happen to your business if the outcome to the critical asset "happens"

Confidentiality
• Disclose sensitive information
Information Security Objectives
Availability
• Lose important or sensitive information, hardware, software
• Interrupt access to important, software, applications or services
Integrity
• Modify important or sensitive information
Asset
… results in …
Impact
Business
CISA
CYBER+INFRASTRUCTURE
18

**018 So what we really want to do is want to step back and think about how it is that we're going to assess how we feel this pain, and we can go through what's called a business impact assessment. Now, this is largely going to be a qualitative assessment and it's what's going to happen if you were to have an outcome in a business, how would I feel the pain? That's classically how you're going to ask that question. Like I said, it may be qualitative but maybe, ideally, you're able to put a quantitative number to it.

Business Impact Assessment Delivers Value for Your Efforts



Business Impact Assessment

Delivers Value for Your Efforts

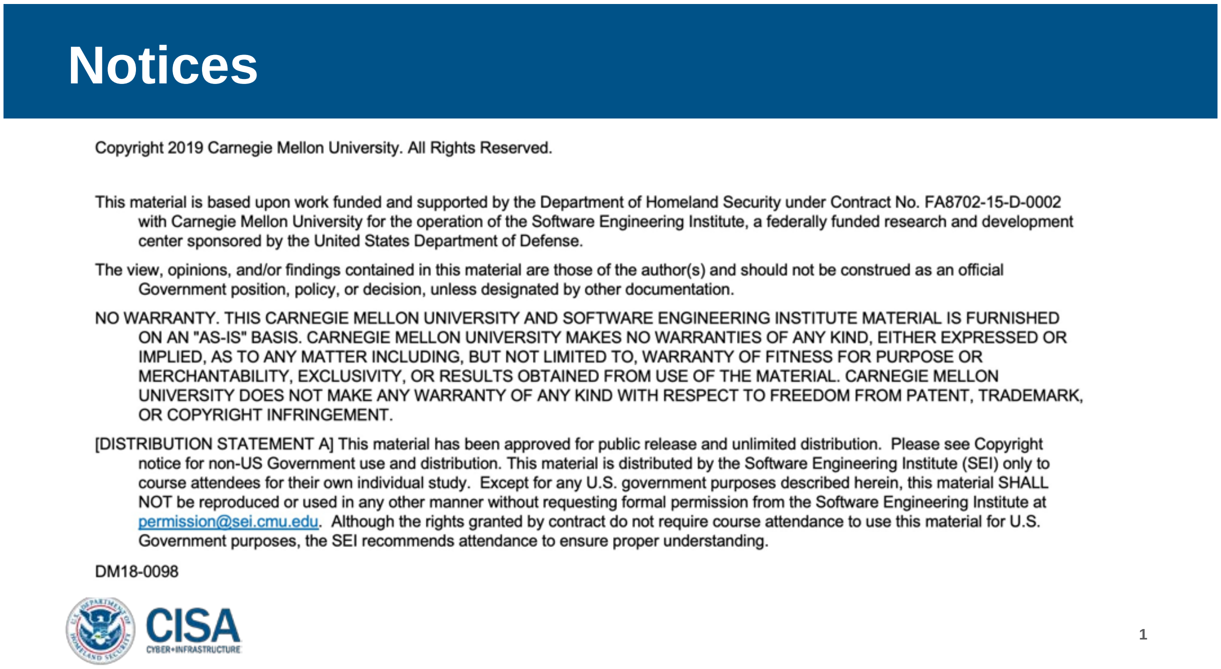
- Serves to prioritize risk management
- Provides basis for the levels and types of protection required
- Provides basis for business case development when coupled with asset valuations

CISA
CYBER+INFRASTRUCTURE

**019 Either way, what you want to do is you want to understand what value you have in that asset to determine how the impact is felt. This is going to help in the end because what you're going to do is you're going to use it to help prioritize the risks in your portfolio, and it gives you a basis for how it is that you're going to categorize and understand where you're going to put security controls that are necessary and how you're going to allocate

resources to establish those controls.
So you're actually, if you think about
it, you're putting a business case to
this risk management process now.

Notices



Notices

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

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.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution. This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study. Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu. Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

DM18-0098