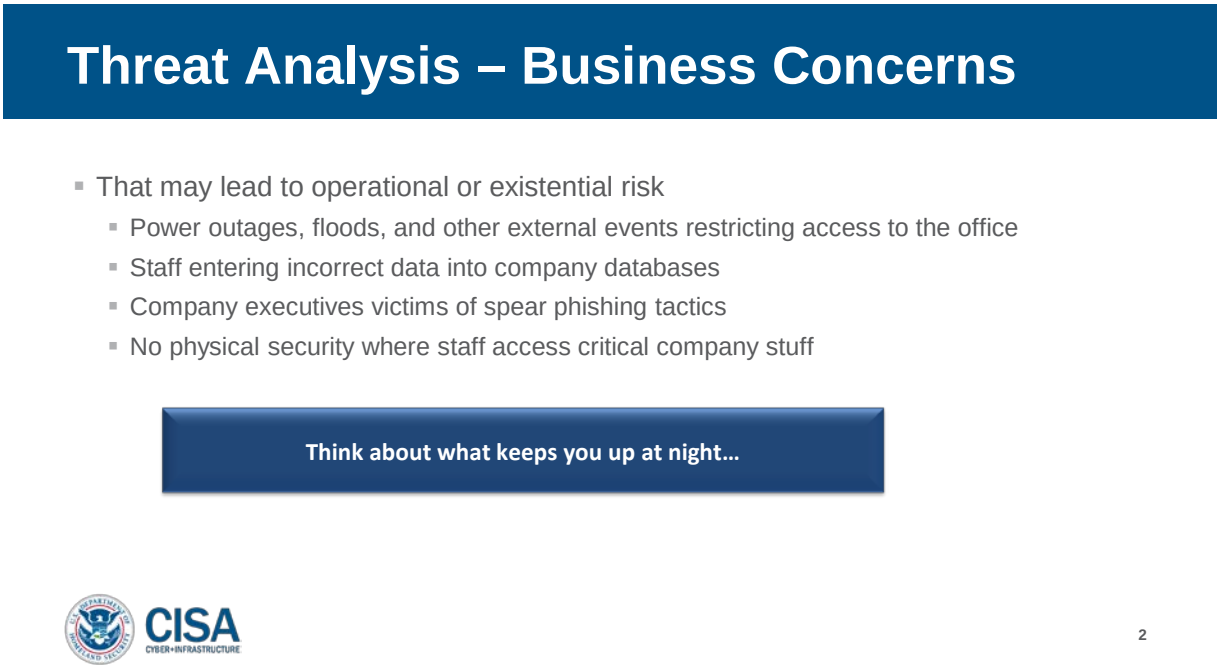
Threat Overview

Table of Contents



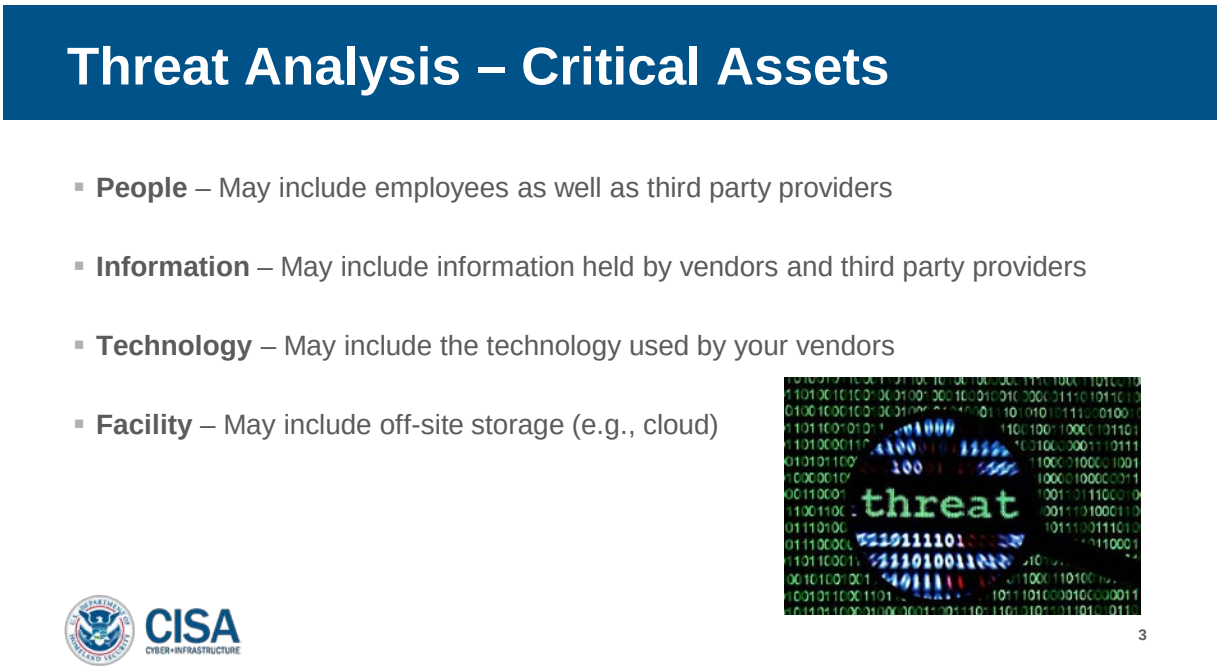
**002 Instructor: So let's start out with what threat analysis actually is. This can be summarized in one easy question you may ask, and it's thinking about what keeps you up at night. So I challenge you next time you go to speak to your manager, to any given executive, as a quick way to get to understanding what uncertainties loom in people's minds, and by the way, it could be any variety of things. It could be maybe some force majeure type instance, power outages, floods, things that would actually keep people from coming to the office or actually delivering on the products they're expected to deliver.

It could be an issue of malfeasance. Maybe you have personnel who are insiders who have access to the system and maybe they do something that's maybe not

necessarily appropriate for the system. Maybe they violate integrity and they actually change data that you wouldn't necessarily want changed. Or maybe it's just a matter of ignorance.

Also, you may have some executives and/or maybe even staff, that open up phishing emails. Clearly this could be a challenge, and it's something that maybe is somewhat benign, because, let's face it, some of these phishing emails can be really good lately, and when you open them up, they think that they're actually getting to take part in a survey that they really feel passionate about, but at the end of the day it's still going to be a threat. So you have to be mindful of these things.

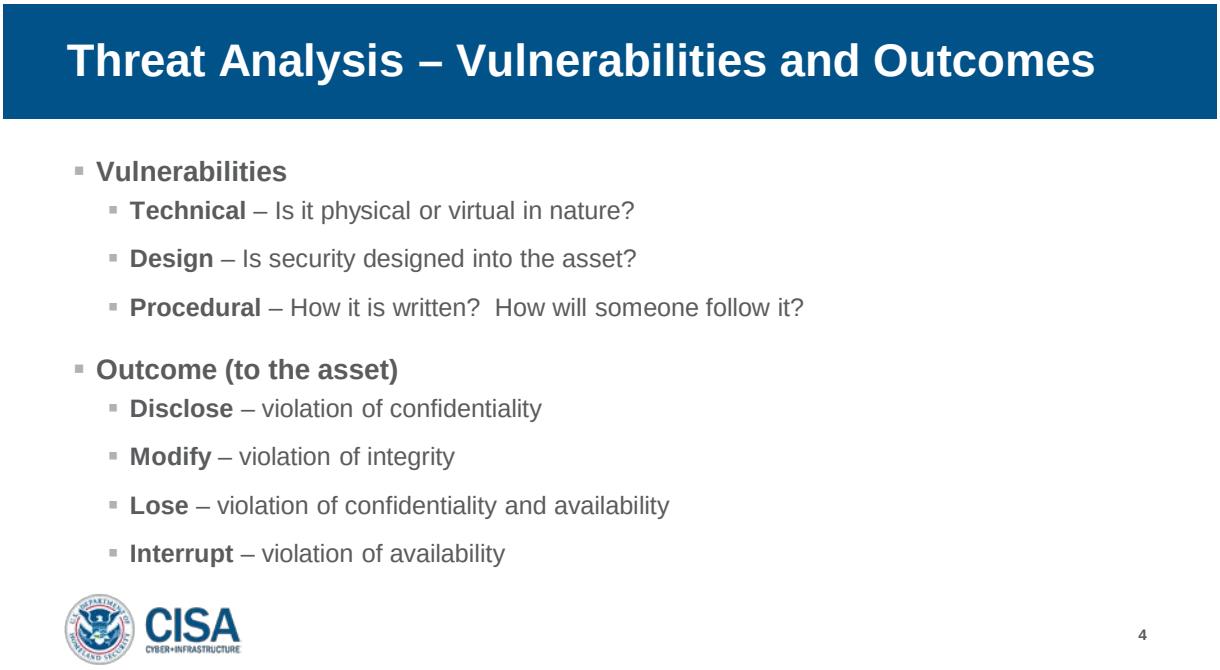
Threat Analysis – Critical Assets



**003 So along those lines of what's keeping you up at night, you also

want to frame that same question along what are the critical assets that I have most concern for? If we go back and think about the services that support the organizational mission and what I'm delivering in terms of objectives, I have four fundamental categories of things, assets, that would be supporting the delivery of those services. It may be people who are working on it, and by the way, those people may not just only have the skillsets, but maybe they have information or something that they do that's important to that process that would be difficult to just find another person to do that same piece of work.

Maybe it's information and the data related to it that builds, that supports that information. Maybe it's technology, computer systems, things like that. Or maybe it is a facility that houses said systems, and in all cases when you talk about these categories, you want to always think about third-party providers. Organizations that are external to your own that are providing you elements of that critical service that if you lost them, ultimately your work and your productivity may be put on hold or impacted.



**004 Okay. So you may also want to think about this threat analysis in terms of vulnerabilities and outcomes, and there are certain types of vulnerabilities that we may want to think about here. Technical vulnerabilities, for example, they may look at the actual vulnerabilities of a computer. Now, it's not just the physical computer that may be subject to high humidity levels, or maybe even an electrical fire. But there may be virtual attacks on that as well.

You may also want to think about the design. Is there security designed into the actual assets that I own? If you think about it, this may be in terms of assets in terms of programs or systems. You may also think about vulnerabilities in terms of what is it that my people do on a regular

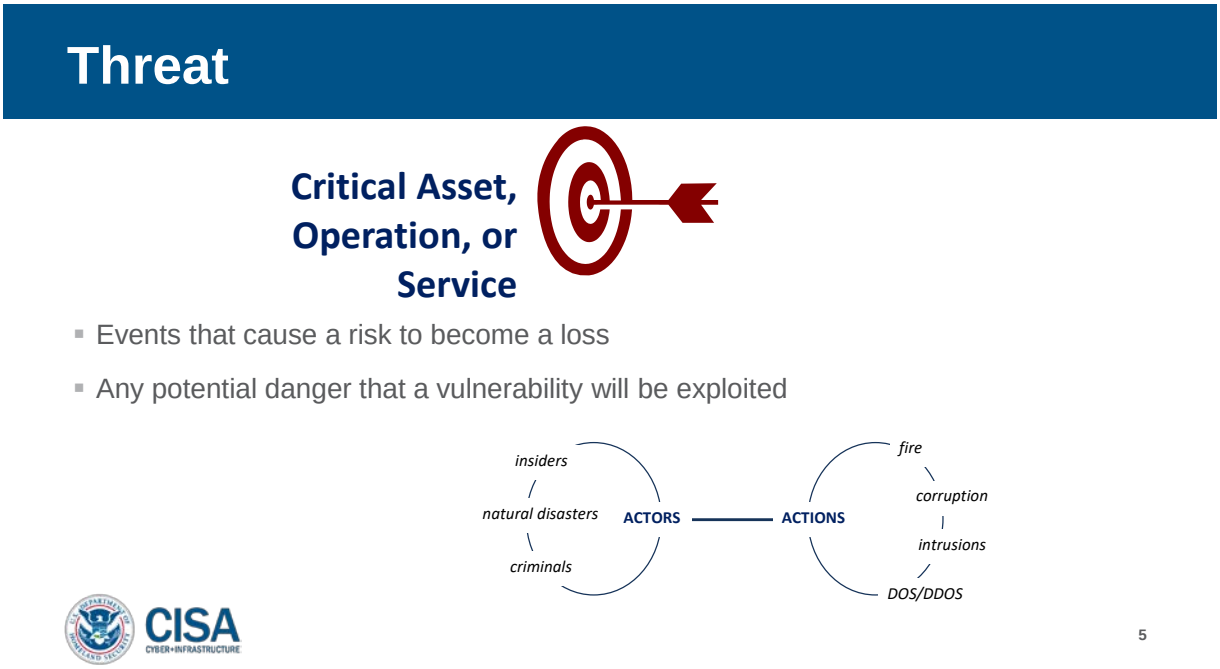
basis? What is it they do that's procedural? How are those procedures written? How are people trained in it? Do they follow the procedures and do they do what's expected of them? So you want to think about that as well, where there may be lurking some vulnerabilities.

Now, you also want to think about these assets again in terms of, "What are the possible outcomes that I could realize if a risk were to come to fruition?" For example, let's go back to the data and information. What if I were to disclose information? If a threat actor wants that information and can leverage it against me, then clearly, I have an issue of confidentiality that I need to be concerned about. Similarly, what if I have a threat actor that wants to modify that information so that way it impedes my enterprise and the ability for it to deliver what I need to do? This would be a matter of integrity that we need to focus upon there.

So just as much as we thought about vulnerabilities, we also want to think about outcomes, and we want to think about those assets and what could happen to them. Think about that information that I was talking about before. If it were to be disclosed, for example, and my threat actor would be able to use that information against me in such a manner that it would impact my organization negatively, then that's an issue of confidentiality that I really need to be focused upon. What if it is the case that a threat actor may be

able to act upon information to change it such that it impedes my operations? Now, this would be a matter of integrity that I really want to focus upon as well. That could be a similar outcome.

Another one would be what if I were to actually lose that information and not be able to get it back? Then I might have an issue of availability, where I won't be able to actually use that information to actually deliver the critical services that I'm looking to do for my--in accordance with my objectives, and in all cases, if I have maybe some kind of interruption, which be strictly an availability issue again too. What if it's that I get, say, ransomware or something to that effect, that actually brings my system to its knees and I wouldn't be able to actually use the assets at hand?



**005 So let's dig a little deeper in this threat idea. Now, threats can be exciting. I mean, the word itself is exciting. You may also think about this almost like a classic mystery game, right, where you want to actually know, "Who done it?" That could be, in a sense, a threat. It can be exciting in a sense too that you're not just thinking about the threat actor but you're thinking about the actions that they need to take.

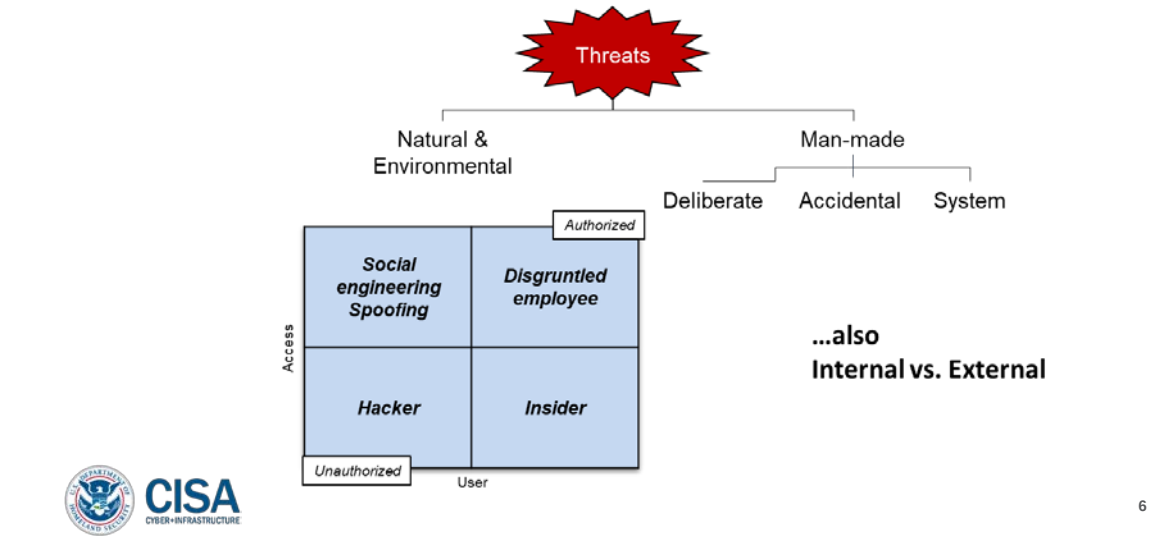
So once again, let's go back to ground zero. We're thinking about the critical asset or operation or service that we need to deliver, but now we've actually turned around and we're starting to think about, "Okay. Who actually wants to disrupt either the confidentiality, the integrity or the availability of those assets, and what's their motive, and what are

they trying to succeed--what are--succeed in? What are they trying to achieve?"

So we want to start thinking about those events. On the actors, we could think about it in terms of people who are inside our organization. We can think about the force majeure idea, a natural disaster, something that we can't control. We might want to think about cyber criminals, and they're going to take certain actions, right?

A natural disaster, for example, could be a lightning strike that turns out to be a fire in my organization. I could have criminals that are--or insiders even that decide that they want to use or exploit the information or the assets that I have for some form of corruption. Maybe an external actor's looking to intrude my system. There's also this idea, like availability, like I said, with a denial-of-service type of attack.

Categories of Threats

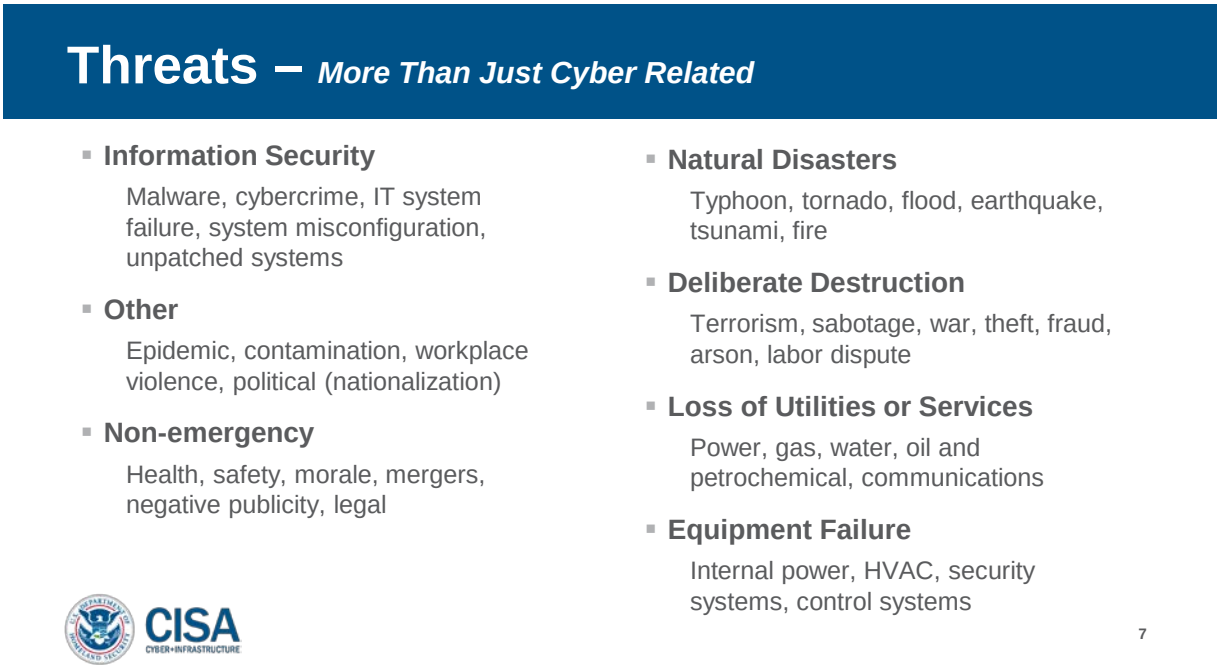


**006 So how do we go about categorizing these threats? We've already kind of hit upon this, but I want to really drive it home. You have this natural environmental threat that could be taking place. I think that's quite clear. Classically we think about addressing those risks related to those threats with insurance. If we all here are homeowners or at least we drive cars, we know that that is a possibility. We usually transfer that risk away using homeowners' insurance or auto insurance, if we're drivers.

But then there are these manmade threats. They may be deliberate, or they may be based completely out of ignorance, and in that case, it'd be accidental. Or maybe it's a system flaw that causes it. In all cases, we

want to think about, for example, the user and what kind of access they may have to the system, and it establishes a spectrum if you start thinking about it, from one end of spectrum the user's not authorized, to another end of the spectrum where they are authorized to use the information. But then again, if their access is high and they're authorized to us it, they can still be a threat actor. It could be a disgruntled employee, and this is true in regards to insider threat.

Threats – More Than Just Cyber Related



**007 So some threats can be more than just cyber related, and the reason why I'm talking about this slide here, and want to focus on the fact that there are threats outside of our IT cyber paradigm, is the idea that a lot of these threats can be interdependent of each other. In

other words, we have some threats that may act upon the organization, and there's a interdependency in those risks that if I have one that's going to happen, then maybe it could affect another.

Let's take for example a hurricane that comes into area. Clearly a terrible natural disaster, and suppose my data processing center is located right on the coast, right where the path of that hurricane's going to tear through. So not only do I have a threat with respect to losing that facility, losing the capability that facility, but I may also have employees that are in jeopardy. I may have my business that is high reliant--highly reliant upon that facility actually delivering on the service that I need.

We may think about this in terms of other things. We think about, for example, equipment failure. Classically, once again, if I have a hurricane coming through an area and I lose power because of said hurricane, there's multiple or cascading risks that are taking place there, and I have to think about all of those.

DoD Scenario – Revisit

What Keeps You Up at Night? How to Think About Threats...

- Naval battlegroup deployment examples
  - The threat landscape is broad.
    - Kinetic threats
      - Adverse forces seeking a shooting war
      - Shipping traffic
      - Weather
      - Navigation hazards
    - Cyber related threats
      - IT system failures/Equipment failures
      - Malware
      - Sabotage
    - All other threats
      - Adverse or ignorant insiders
      - Morale

CISA CYBER+INFRASTRUCTURE

8

**008 So we have a scenario where we're a battlegroup, a Navy battlegroup that's deploying, and the commanders are staying late up at night while this carrier and a cruiser and some destroyers and some--a submarine and maybe some aviation assets are going to sea, and they're going to a bad place. Clearly the Navy is not really going to be a war fighting Navy if it's not going to at least a threatening place. You really need to think about that threat landscape, and this is probably what keeps those admirals up at night, right? They think about, "Hey, what are the kinetic threats that I may have in an area?" and by the way, it may not necessarily be an adversarial force. Maybe it's just shipping traffic. Maybe it's weather.

Another thing they may want to think

about would be cyber threats. So I challenge you to think about that as well, and by the way, it may not be necessarily a sailor clicking on a phishing email. Maybe it's an insider who's thinking of actually corrupting one of my control systems to my engineering plan. There are other threats too that you may want to think about that may come into play here. That may actually build to a threat that may actually impact your organization in a way that you wouldn't suspect. Suppose my workforce morale is really low. This could actually be a threat. I could have a sailor who's disgruntled because of said morale being low, and they could actually become an adversarial insider threat actor.

Notices