Risk Mitigation Strategies

Table of Contents

Risk Mitigation Strategies

**022 Instructor: Now I want to talk about risk mitigation strategies.

Build a Contingency Plan – Preparing for the "Dark Day"

- Compare costs of disruption vs. recovery.
- Establish a plan of action for the expected highest and most likely risks.
- Concentrate on the business objectives.
  - Risk is NOT threat – it is an understanding of what is important to the business.
  - Threats, vulnerabilities, controls, and impact are all factors.
- Prioritize security implementations based on risk.
  - There is probably not enough time or resources to implement everything.
- Good security is about multiple layers of protection—**defense in depth**.

CISA CYBER+INFRASTRUCTURE

23

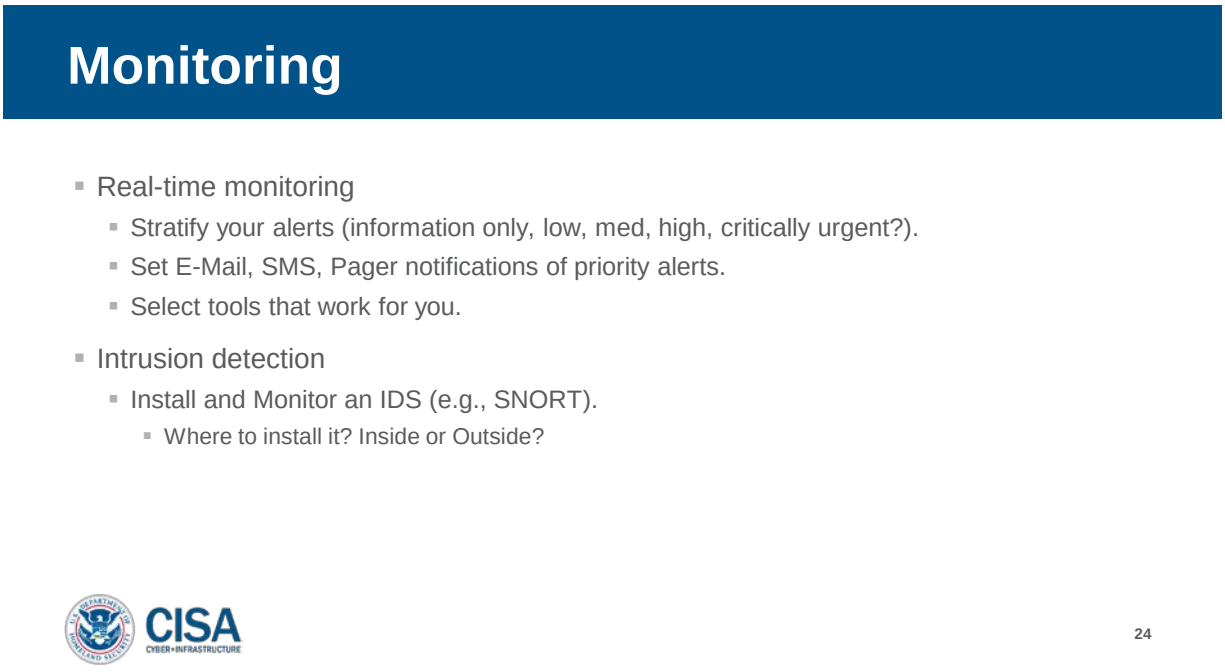
**023 But before I do, let's recall that there are four different strategies for responding to any given risk. You can accept the risk, you can transfer it, you can avoid it altogether, or you can take action to mitigate it. Now, by taking action to mitigate it, it means I'm actually going to invest resources so that way I can address that cold, dark day if it were to happen. In this case, a type of mitigation plan would be contingency planning.

Now there's a difference here. I could have a business disruption, versus I could also have recovery of operations that need to take place. A disruption would be suppose I have a manufacturing facility and I'm producing widgets, and I usually produce ten an hour. If I have some kind of disruption to operations, I

only have five an hour that I'm producing. That's a really different scenario from where I've actually lost production altogether and I need to recover for no widgets an hour being produced. I want to think through each of these scenarios when I'm developing that contingency plan. I want to have a plan of action, a series of steps that I may have to take in case this risk comes to fruition.

Now, to do that, if I have nowhere else to start, I want to focus on what my business objectives are. Remember, what I'm really trying to do is I'm trying to prepare that a threat is going to exploit a vulnerability and my organization is going to feel pain. So in this case, I want to think about all those factors, but specifically I want to think about that pain. I'm feeling it. How best do I stop the pain, and how best do I get back into action?

Now, you also have to remember, if you're establishing these contingency plans, they need to be realistic. You only have a limited amount of time and/or resources to get your operation back up and running, so you really want to think about maybe layering your security, layering your plan, such that if something were to happen, I have multiple steps that I may take, each one putting me back on the path, or at least a little bit closer to it, so that way I can just get operations up and running at least in a more cost-effective manner as well as a rapid manner. We would call this notion a defense-in-depth.



**024 Once I have these in place, another mitigation plan I could have, or another strategy I could use, is how am I going to think about monitoring this risk. How am I going to know that the plans that I've implemented are actually being effective? How do I know if the risk is actually even coming to fruition?

Now, there are different ways to think about this, and before I even get to what's on this slide, I want to talk a little bit about what a key risk indicator is. Maybe you've heard about this, a KRI, and what I'm really looking for are road signs. If I'm trying to travel from Point A to Point B and I need directions along the way, I'm going to look for nice big signs that tell me that I'm almost there. Risks are no different. They may be inbound, and you may need

to know that they're going to happen. Some of them may be subtle. Some of them may be very obvious.

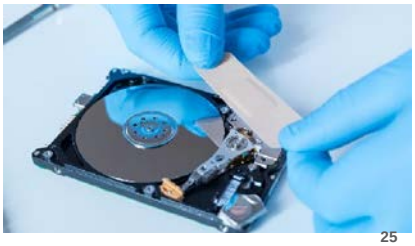
Let's take, for example, a hurricane. Suppose I have a hurricane coming up the coast. There's a very clear indication that it's coming with high winds, rain, things of that nature. Those are all indicators that I can clearly monitor and know that I have risk that are going to come to fruition, and I'm going to have to take action. That said, I may want to stratify those alerts. It's not just that I'm looking for the winds to actually show up at my front door. No, I'm looking with radar out at sea to see that that's coming. So I have, once again, this defense-in-depth strategy where I can see where things are coming closer and closer.

You can do this in terms of IT as well. Suppose I have priority alerts. Whatever you do, you have to make sure that the tools that you have work best for your people. Another good example of this would be intrusion detection, suppose an IPS or IDS. But you got to really put some thought to, "Hey, where am I going to install this?" And, to be honest with you, if I do, how strict am I going to make the filters that they're looking for? I don't want my IDS or IPS to actually inhibit operations.

Scanning and Patching

- **Vulnerability Scanning**
  - Schedule regular scans using an updated engine.
    - Web application, operating system, third party application scanners are all available.
- **Patching Systems**
  - This is NOT a silver bullet – but helps keep some intruders out.
  - Use automatic updates where available.
  - Vulnerability scanning can identify what is missing.
    - Do not assume that because you "installed" it, it actually took.
  - Remember to include third party application updates (adobe, flash, firefox, etc.).

CISA CYBER+INFRASTRUCTURE



25

**025 I can also do a lot with scanning and patching. I can think about where I have gaps in my system, and I can do vulnerability scanning. There are lots of different tools out there. Regardless of whatever one you use, it's highly suggested that you keep them updated such that they know what the most current vulnerabilities are in your systems.

You can also be sure that you have to patch your systems, and you have to do it quite regularly. Now, it's not a silver bullet, but to be honest with you, at least it keeps out the riffraff, if you will. It keeps the low-level players out that are taking advantage of vulnerabilities that are largely already known.

Sometimes you'll have applications and systems that will use automatic updates. I encourage you to use those wherever they're available. Also you can have vulnerability scanning that can tell you maybe what is missing from your system. Maybe you haven't installed a patch correctly yet. Remember also that if you have third-party providers that are working for you, or if you have assets that they have that they're using to make their operations go, you want to make sure that they're doing their part too in terms of understanding what their vulnerabilities are and make sure that they're patching their systems as well.

Backups and SLAs

Backups and SLAs

- Data backups
  - Backup everything that is “important” according to the business plan.
  - Test backups to make sure they work.
- Service level agreements (SLAs)
  - Services
  - Facilities
  - People
  - Do they meet requirements for availability?
  - Use clear language and obtain legal help.

CISA CYBER+INFRASTRUCTURE

27

**027 So another mitigation that you may use here are backups and service-level agreements. A data

backup-- you can think about that as you have all the information that you have in your enterprise and you're just copying it in another place, so that way if you lose your system you can go back and get it. There's a number of different strategies here, such as using RAID and things of that nature, but in general, what we want to leave with is the idea that you have a business plan that tells you how you're going to actually establish making those backups and how you're going to use them if the dark day comes and you have to recover using them.

You may also think about third-party providers that you have that are helping you in delivering your critical services. So you're going to establish agreements with them such that you know specifically what services they're delivering, what facilities they're doing it from, what people they're using. You want to be very specific, or at least as specific as possible, so you can control the amount of risk that not only they have, but that you have that you're working with them. You want to make sure that you're going to get help from legal counsel such that you have the proper language in any of these service-level agreements such that you get the service that you're looking for.

Establish Relationships

- **"Bubba Net"** (Bubba = Friend, Net = Network)
  - Establish professional networks.
  - Know **who to call** when assistance is needed.
    - May include federal and local officials
- Develop information sharing relationships
  - Expand your sensor grid
  - Find new threats and vulnerabilities
  - **Share** attack indicators and information.

- Media / public relations
  - **Invite media** to discuss best methods of communicating with them.
  - Build a **communication plan** of how to respond in given situations.

CISA CYBER+INFRASTRUCTURE

28

**028 Now, it's not just about having technical solutions. Mitigation could easily be about relationships, if you think about it. We talked a little bit previously about a "bubba net". A bubba net is really just nothing more than having a friend, somebody within the industry or somebody in another organization, that you know is familiar with the technology that you may be using as well, and maybe you're familiar with theirs. You can call and share best practices.

Now, we could call this a bubba net, but to be honest with you, it's a professional network as well. Establish these professional networks such that you know who you can call at any given time. By the way, it may not be necessarily within your organization. It may be without. It may be within your industry. It may

be in the public and/or the private sector.

You also may want to consider how you can share information. You really want to be able to understand what are the wolves outside your gate in terms of threats, and maybe you have partners that have much better sensors to understand what those threats are. If so, you certainly want to establish a relationship there if at all possible so that way you can get that early warning that they have as well. They could also be identifying new threats and vulnerabilities that you may not necessarily be familiar with, and vice versa. So be sure to share back if you find it as well.

Another thing you want to think about is how you can leverage the media and public relations to really help you in your journey if you should have that cold, dark day arrive. You really want to keep the mindset that you want to keep your customers informed such that your reputation is not damaged. So, you're going to have to have some sort of relationship with the media so that way you understand how to communicate with them, and maybe even have a plan so that way you know if you do have a risk that comes to fruition, you know specifically what to say to them and who's going to be saying it.

Awareness, Training, and Education

- People are typically considered the greatest source of risk to an organization.
- Providing appropriate training can have significant impact in mitigating risks.
  - Awareness – involves reinforcement that security supports the business/mission by protecting valuable resources
  - Training – involves skills taught to be used in performing security tasks
    - Most effective when targeted to a specific audience
  - Education – involves in-depth teaching for security tasks requiring expertise

CISA CYBER+INFRASTRUCTURE

29

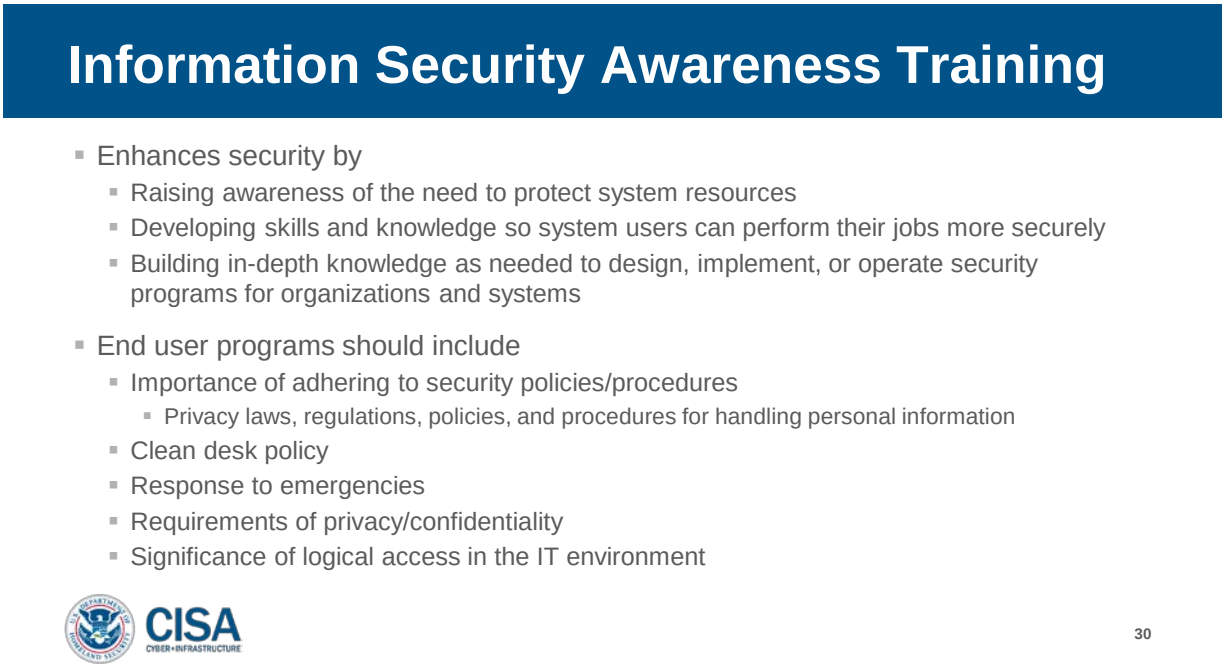
**029 People are a critical asset to your organization, and it's really important that they're aware of their responsibilities and what they're accountable for and the role that they play in managing risk in your enterprise.

Now, there are different flavors of this. You can make them aware with awareness campaigns. You can actually sit them down and in-house give them some kind of training. Or you can send them outside the organization and get a deeper dive in some sort of education. This would be like a graduate degree, for example.

So we want to think about any of these three strategies either individually or they can be done in tandem, maybe together. Maybe I

run some training along with an awareness campaign. Maybe I have some plans to send people to get additional education to bring information back and share it within the enterprise. Think about how you can layer this such that your resources are optimized.

Information Security Awareness Training



**030 So let's talk about this information security awareness training. Really what you want to do is you want to get the awareness up in your enterprise so that way everybody knows that they are playing a role in protecting the resources of your organization, your assets. You want to be sure that they have the skills and the knowledge necessary that they can do their jobs, such that they're not introducing new risk to the organization, and this is really kind of

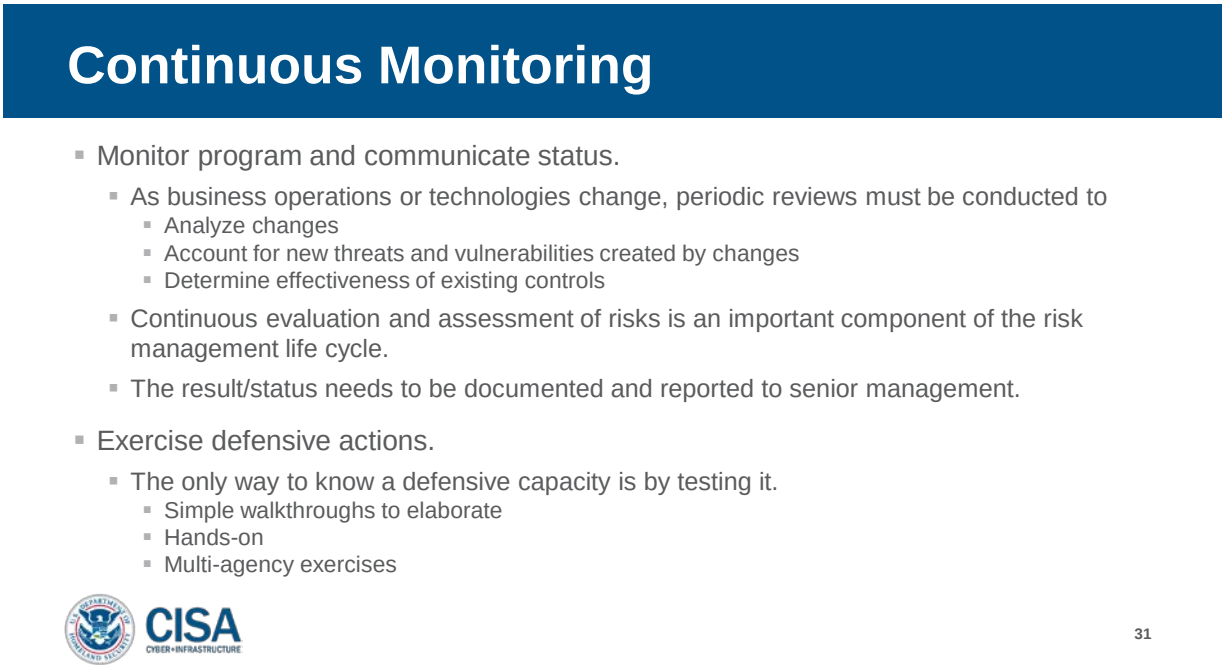
harder than it sounds. But what you really want to do is build the base level of knowledge in your organization such that everybody knows at least that you have a security program, and the fundamentals of how to adhere to it. This comes with very clear policy writing. You want to make sure that everyone could read your security policy, your goals and objectives, and understand them at a level regardless of what they bring to the organization in terms of technical expertise, and/or even literacy.

When you're establishing information awareness in your organization, you really want to have the end-user in mind. As I said before, you really want to have clear policies and procedures to make sure that they can be informed at a level that they can understand. For example, you may insist upon a clean desk policy. Be specific in what you mean. It may not mean necessarily that everything comes off their desk in a day, but certainly all documents and any critical assets would be locked away at the end of their day. They should know how to respond to emergencies-- and by the way, it's not just about giving that awareness training. You're going to have to drill them. Make sure that they're adhering to the policy by running drills and tests on them so that you can see that they what they're doing when the time comes.

They may have to be aware of confidentiality or privacy rules related

to the assets that they're using. They may also have to think about the kind of access that they have within the environment they're in, and how significant that may be. It's one thing to come in, log in a system, and check your email. It's a whole other thing to look at a proprietary email and take it out of the organization and radiate it out to the public, which would not be a good thing. They need to understand those distinctions.

Continuous Monitoring



**031 So, I have to keep my mind set to the game of managing risk continually, because as I used that example of wolves at your gates, those threats, they're always going to be there. So you're going to have to have some kind of continuous monitoring in play. Now remember, continuous monitoring is not just the

matter of continually looking out the window to see if the storm is coming. You want to actually look for trends and changes in operations. You want to be able to look at the horizon to see any new threats that are coming up, any new vulnerabilities that may exist. So threat intelligence is important, and this goes back to the idea of keeping my vulnerability scanners updated.

You also want to look at the controls you have in place and have effective measures in place that you understand that your controls are being effective. This is not easy. As a matter of fact, before you go out and implement technical solutions, you really need to sit, stop, and think about how you're going to measure that effectiveness. What data are you going to collect? What kind of information are you going to glean from that data, and what are you going to do with it? Who are you going to tell about this information? How is it going to be documented? What is it that your senior management expects to see when they want to hear about how effective your system is operating?

So you want to think about defensive actions that may need to take place as well. The only way you know about this is by testing it. There are different ways you can actually test defensive actions that you have in place. You can have walkthroughs. You can have tabletops. Some of these could be very elaborate. Maybe I actually go out and actually

turn systems off. Maybe I have a parallel system operating where I'm going to run exercises. Either way, the more hands-on you get it, the more effective you're going to find it's going to be, and if you really want to get complex about it, but I'll tell you it's going to have a high return on investment, is when you can get multiple agencies or multiple organizations to play in -- your partner organizations that we've talked about before.

Cost/Benefit Analysis (CBA)

Cost/Benefit Analysis (CBA)

- An organization should consider costs versus benefits when controls and/or countermeasures are planned.
  - If the cost of controls exceed the benefit, the organization may choose to accept the risk instead.
- CBA usually involves a trade-off between security and business operations.
  - Be sure to document assumptions, results, and decisions.

CISA CYBER+INFRASTRUCTURE

32

**032 You may also want to think about how you're going to get value out of the controls that you're setting up. To do this, we're going to do a cost-benefit analysis. Now, you should look at the resources that you're investing and you should also look at the countermeasures that you have that are planned to put in place.

If the cost of what you're investing in the controls far exceed the potential impacts of the risk that you've planned for, then chances are that may not be a wise investment. So you really have to put your business mindset to this and understand that you're actually getting a return on your risk investment.

As you're doing this, it's critical that you document any assumptions that you've developed and that you track the results. And you want to be mindful also to document critical decisions that are made, so that way if the environment, the control set, or the threat, or any element changes, you know how you got to the place where you're at in terms of your control implementation, or your response implementation.

Total Cost of Ownership

Total Cost of Ownership

- When considering costs, the "Total Cost of Ownership" (TCO) must be addressed for the full life cycle of the control/countermeasure.
  - This may include costs for
    - Acquisition
    - Deployment/implementation
    - Recurring maintenance
    - Testing/assessment
    - Compliance monitoring/enforcement
    - Inconvenience to users (user downtime)
    - Reduced throughput of controlled processes
    - Training in new procedures/technologies as applicable

CISA CYBER+INFRASTRUCTURE

33

**033 Also, it's not just about

getting the response implemented. There's going to be a total cost of ownership. It's not just, and goes beyond, acquisition, or maybe even the cost related to implementing the system. You may think about that you have to actually train your personnel to know how to use it. That costs money and time. You may also have to think about maintenance that has to occur. This may cost money and time as well.

Now, note that when you have downtime, it may be inconvenient to your users, but it may also be an inconvenience to your customers as well. This could mean lost revenue. That is another critical element you may have to think about.

Notices