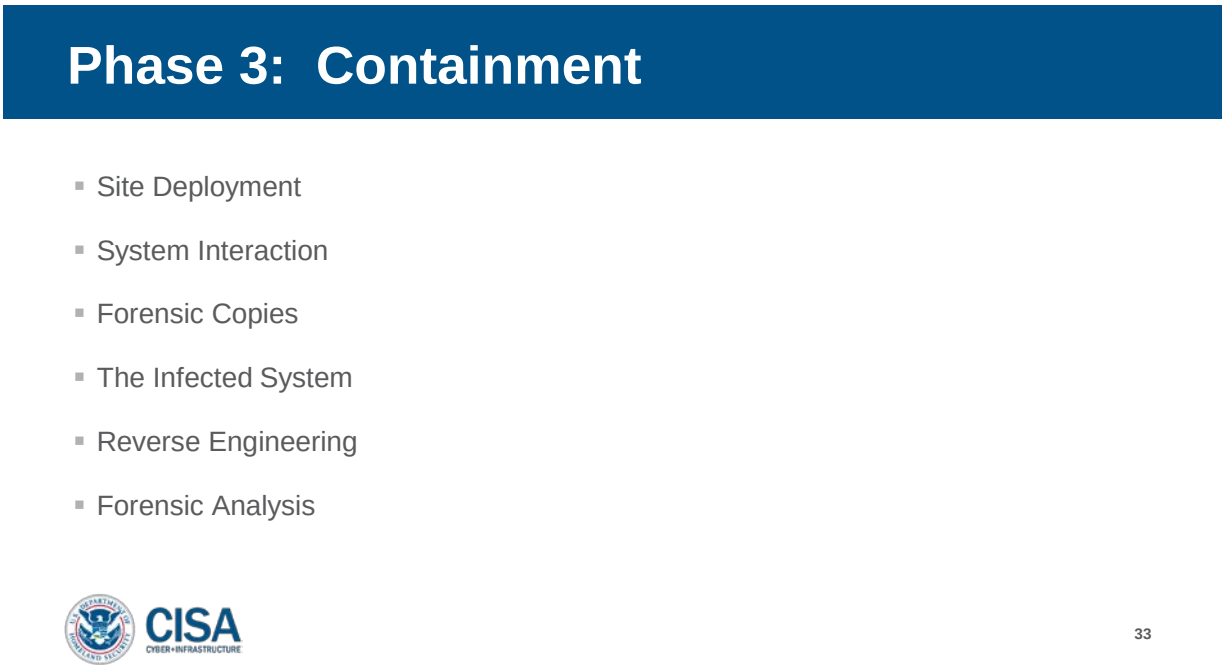
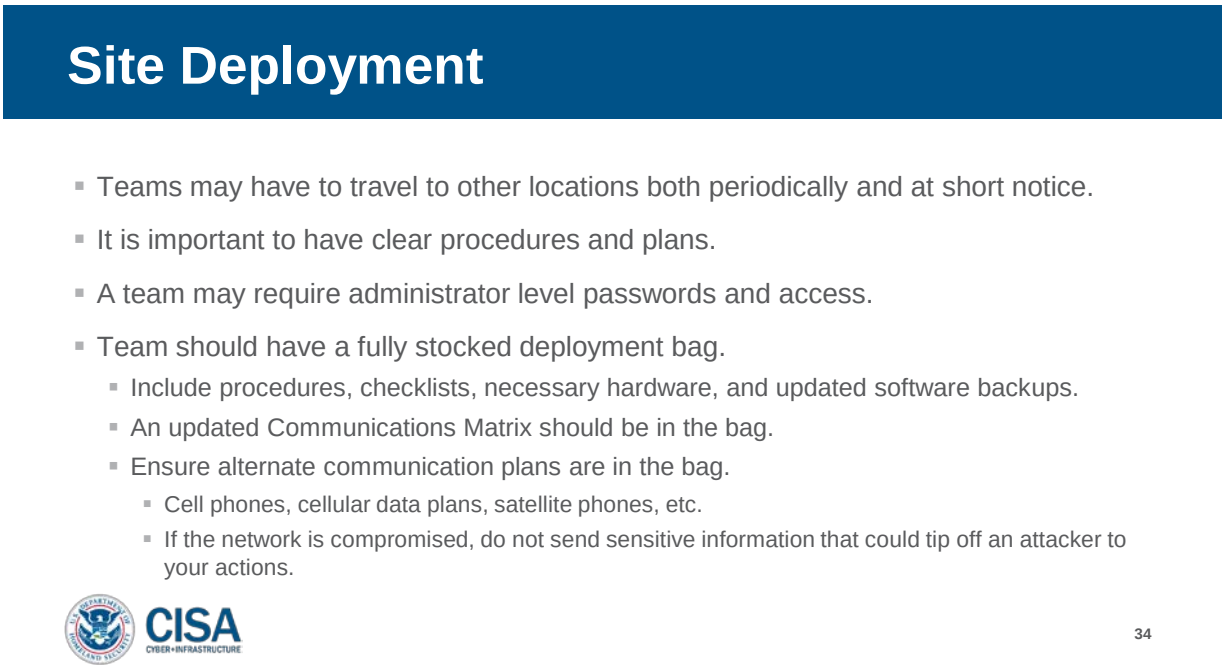
Incident Response Phase 3 of 6 – Containment

Table of Contents



**033 Instructor: So let's move on now to phase three. This is the containment phase. Now, there are couple things you want to think about here. "How are my security systems deployed in my organization?" and you want to think about how these different systems are interacting with each other. How I'm collecting data and how I'm using it to leverage it for forensic information. How I'm actually handling the infected system, and how, in fact, I can recover from that, and then what do I do with that forensic information now that I have it?

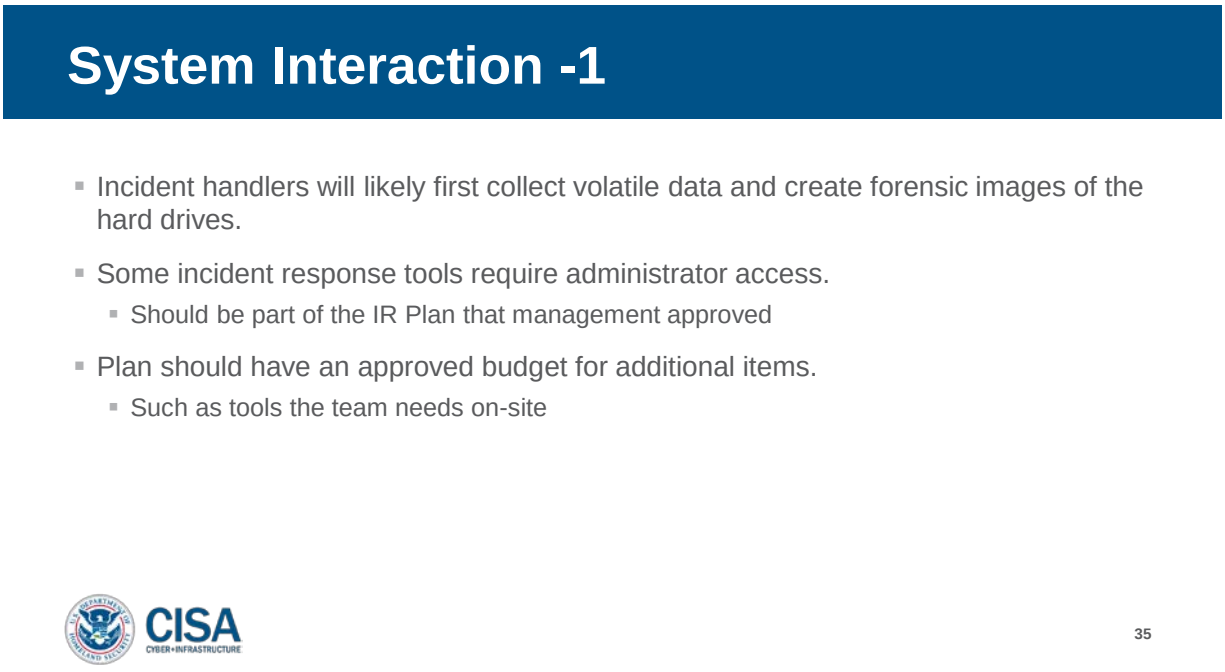


**034 So let's talk first about site deployment. So you want to think about this, that you have an incident response team. Now, remember I said that they might be virtual. They may be placed at multiple locations, maybe even all over the country or the world, or they may be a centralized team that operate in one particular location, and that can be thought of as an away team. They immediately get on a plane, if you will, and fly to that location. Either way, you may have to have a triage team that's actually on the site where the event has actually happened, and they have to have real clear procedures and plans for how to operate until that backup team, that IRT, is there to respond.

You may also want to think about what kind of access that team has.

Do they have administrator level access? Do they have that local administrator access that they need to actually get into the system and do what they need to do? This may also require that they carry around hardware, software backups, checklists, contact lists. All that kind of material needs to be in one location. An away bag, if you will, a deployment bag. They're going to pick that up and carry it to the site wherever they're headed, even if it's within the same building that they're in. It's important to keep this bag up to date with the most critical information and the most timely information.

A good example here is a communications matrix. Think about it. I have people coming and going in an organization at all times. If they leave and the cell phone number changes for the most--the next most critical person I have to call, that matrix is now worthless in a sense, if it doesn't have a backup number on it. So you need to keep looking at this and making sure that that information you have in this deployment bag is the most up to date.

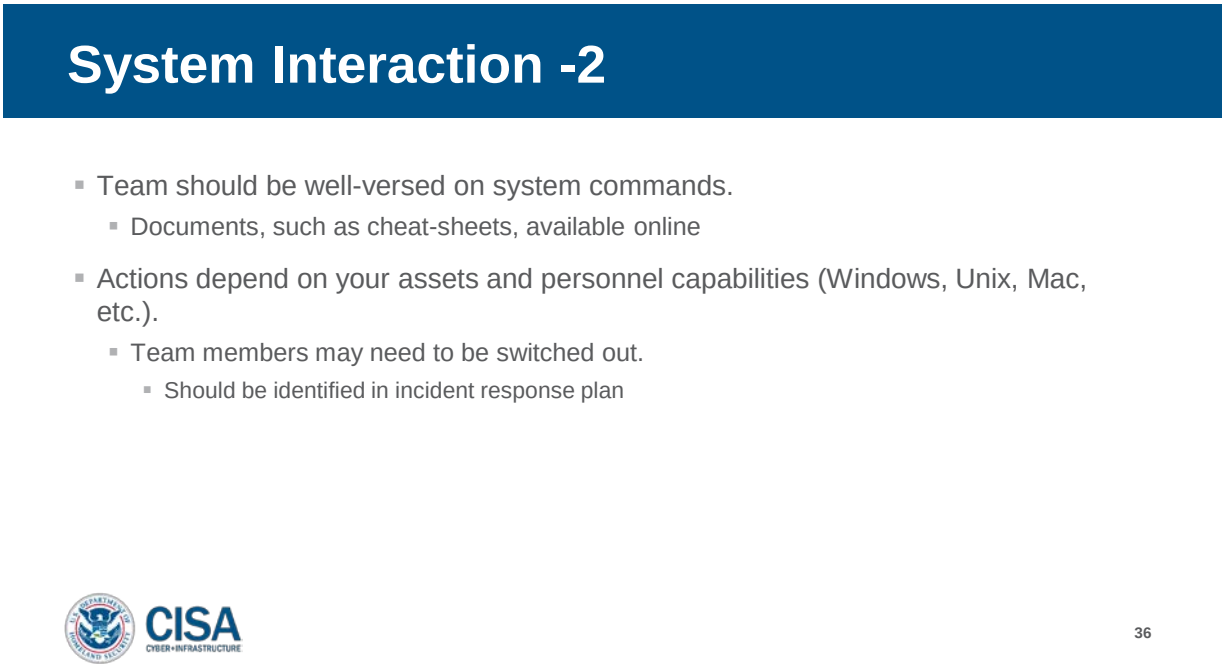


**035 You also have to think about how systems are interacting with each other. Now, you're going to have data that's going to be coming into your organization, and some of this is volatile. Like, it's going to be there and then you're going to have more information that either comes in and replaces it, or it's going to lose its meaning in terms of information that's critical at that moment.

You want to think about how you're collecting that data and storing it for a later date for processing and understanding how things actually went down. You also want to think about that some of these tools require administrator access, and all of this should be part and parcel with what you have in your incident response plan and how it's all managed.

Also, you may want to think about having some contingency money set aside just in case someone has to run out, literally, and buy a--something necessary to alleviate this event. You may also think about it this way too. It may not be someone physically running out the organization. Maybe they actually go buy a commercial off-the-shelf product right off the internet for immediate security right then and there. This could be challenging, but truly, if you've hit that dark day, you're going to need to have those funds in place so that they can take that meaningful action.

System Interaction -2

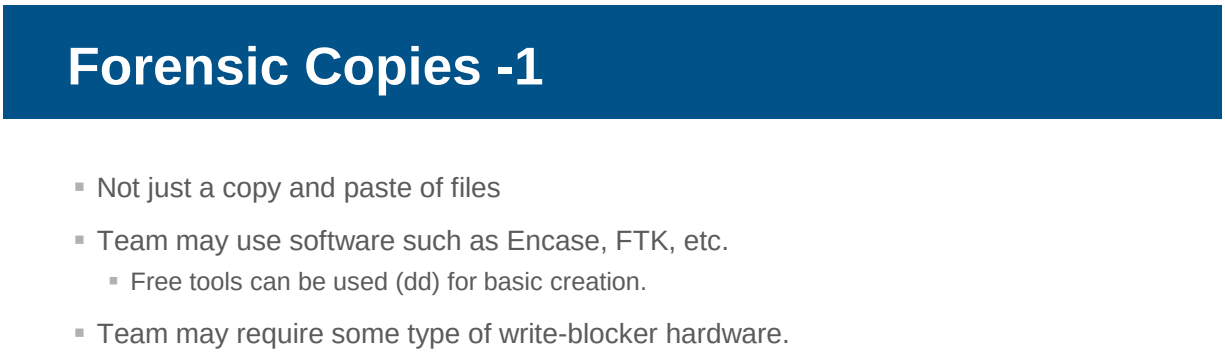


**036 Once again, these interactions need to be understood at the level of the team. They need to know everything, and it needs to be well documented. It's helpful at times though, when people are not perfect,

that they have at least a cheat sheet or some kind of checklist that they can go to and they can refer to make sure that they're doing the right things, even if they had it memorized. Things change. So what they have memorized may not necessarily be the most up-to-date actions that they have to take.

You may also want to consider the fact that people come and go again. So when team members are rotating or being switched out, you need to make sure that they have the most relevant skills and capabilities, so that way you have a well-rounded team, so that way they can provide you a holistic response regardless of the system that may be being used, for example.

Forensic Copies -1



**037 You've collected all this information, and you don't want to

have it just be a copy and paste of what has taken place. This is the actual, no kidding, data that you've collected. Now, there are certain tools that you can use for this, and it's recommended that regardless of what you use that you don' want to change any of that information that went in there forensically. The reason being, is suppose I want to establish a legal case for the event that has taken place, and if that is the case, if I change any of that information, it could change that information to a level and degree that a court will no longer accept it, that I can no longer prosecute.

So for these forensic copies, you want it to have some kind of write-blocker that prevents people from going in and changing it.

Forensic Copies -2

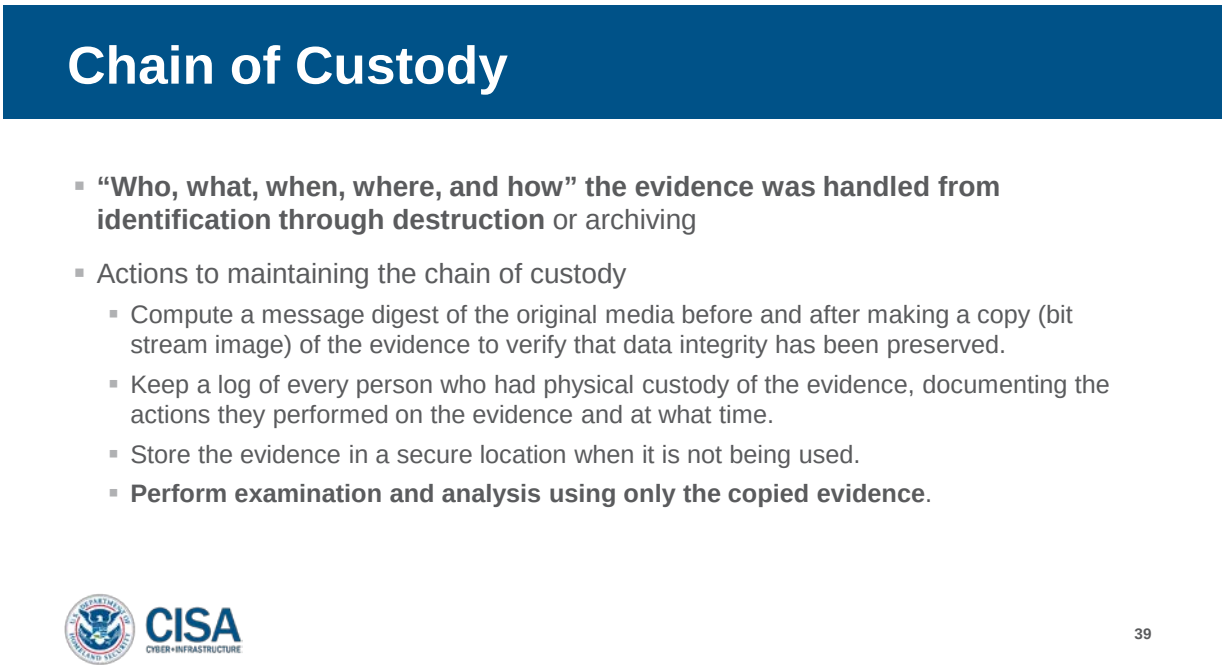
- Important if legal action occurs
  - Even if you do not plan to pursue legal action, follow the process.
    - Benign cases have resulted in instances where a user is actually involved in illegal activity.
    - Cases where a person was accused of illegal activity, arrested and then forensics determined that a hacker had actually done the activity have happened.
- A clear chain of custody must be maintained
  - Legal standing could be lost if specific steps are not taken properly.

CISA CYBER+INFRASTRUCTURE

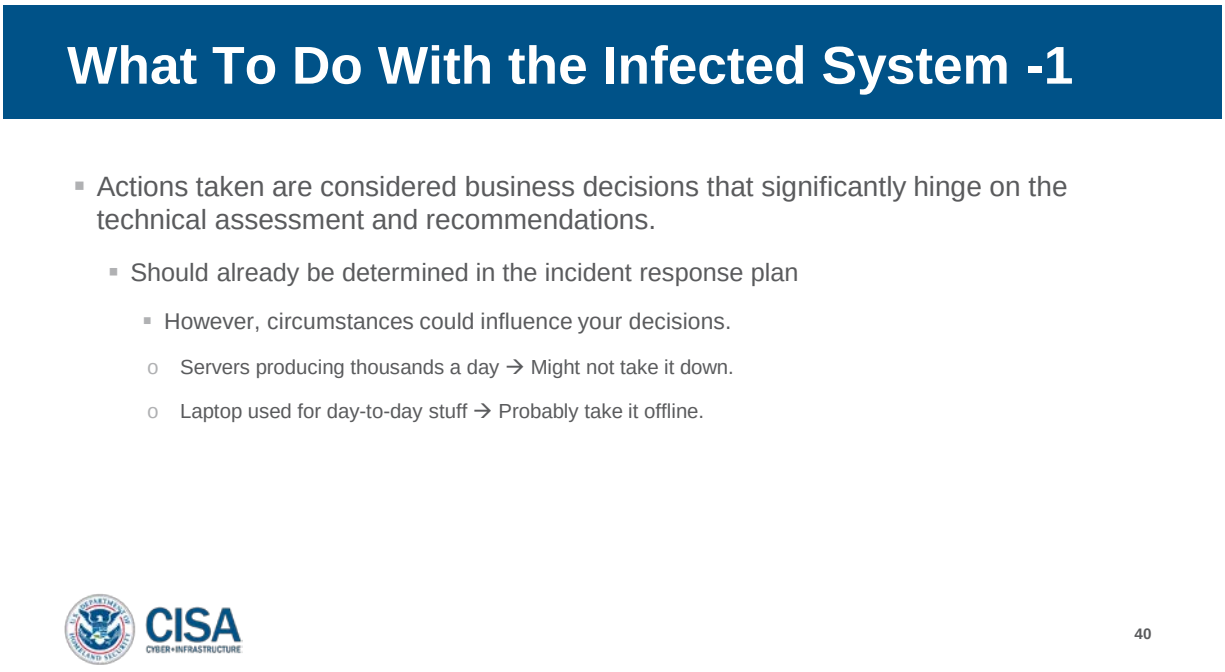
38

**038 Now, the other thing you want to think about here too is to have a chain of custody. So in other words, whoever has that information, it is logged that they actually had it and you have to understand what they did to it and make sure that that's properly documented. That way you maintain that legal standing of that information.

What I would recommend for this forensic information business is that you keep that information in one spot and you make copies of it and use the copy for analysis.

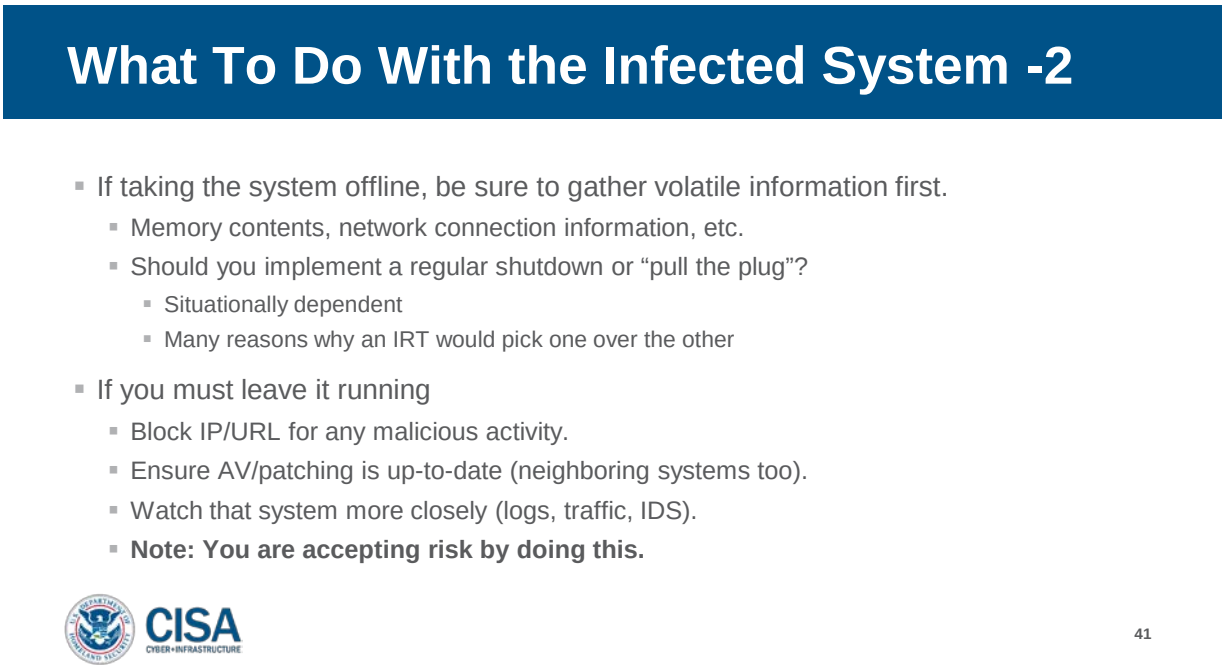


**039 Let's talk a little bit more about that chain of custody idea. This is literally the who, what, when, where, how of that information you have. From cradle to grave too. From when you ingest that information, you actually take it in, all the way through when it's finally destroyed. You want to think about how you're going to actually properly document this. What's your log look like? Where do you keep it? How are you documenting the actions taken with it? And you want to make sure too that the analysis is taking place on those copied forensic files, as I've talked about before.



**040 So now that I have had this risk come to realization, I have an infected system. What do I do? You have to think about this in light of being a business decision. Remember the key here is that I need to keep operations going. So what I want to do is have very clear and detailed instruction on my incident response plan that accounts for multiple decisions that are taking place.

For example, if I have servers that have thousands of transactions going on in a day, I might need to keep that thing up and running to keep my operations going. Otherwise, if I have a laptop, for example, I just unplug it and shut it down, and that way it no longer has any influence on the rest of my system.

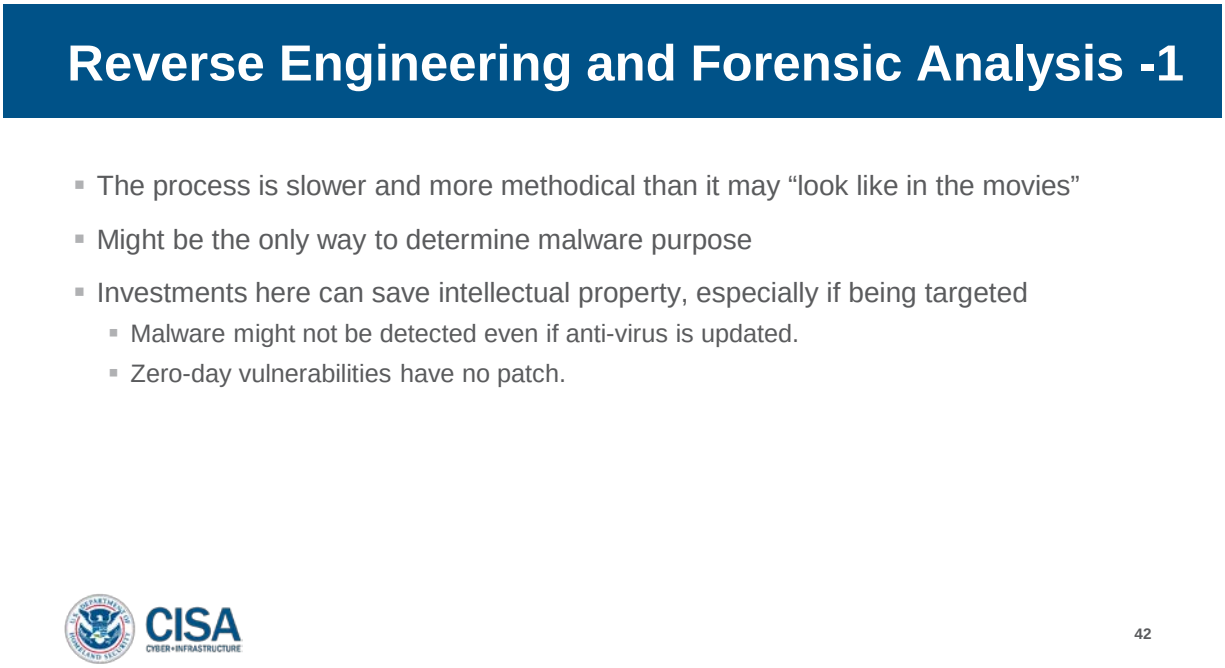


**041 So now you have this infected system, and you're making the decision that you have to take it offline. Be sure to capture any data that would go away once you hit the button or once you pull that plug. If you have to leave it running, you want to consider how you're going to block any malicious activity from going on outside of that spot where you found the actual infection. You want to make sure that the rest of your systems around that, that particular infection, are patched and up to date.

You also want to make sure that all the information you have in the system is being continually monitored to make sure that the, if the infection has spread, you're aware of it and you can take additional action. Note that if you're not unplugging the

system and you're going to keep operating, there is significant risk related. I would recommend that not only you document the decision but you also vet it with your management team so that they understand the risk that's being taken.

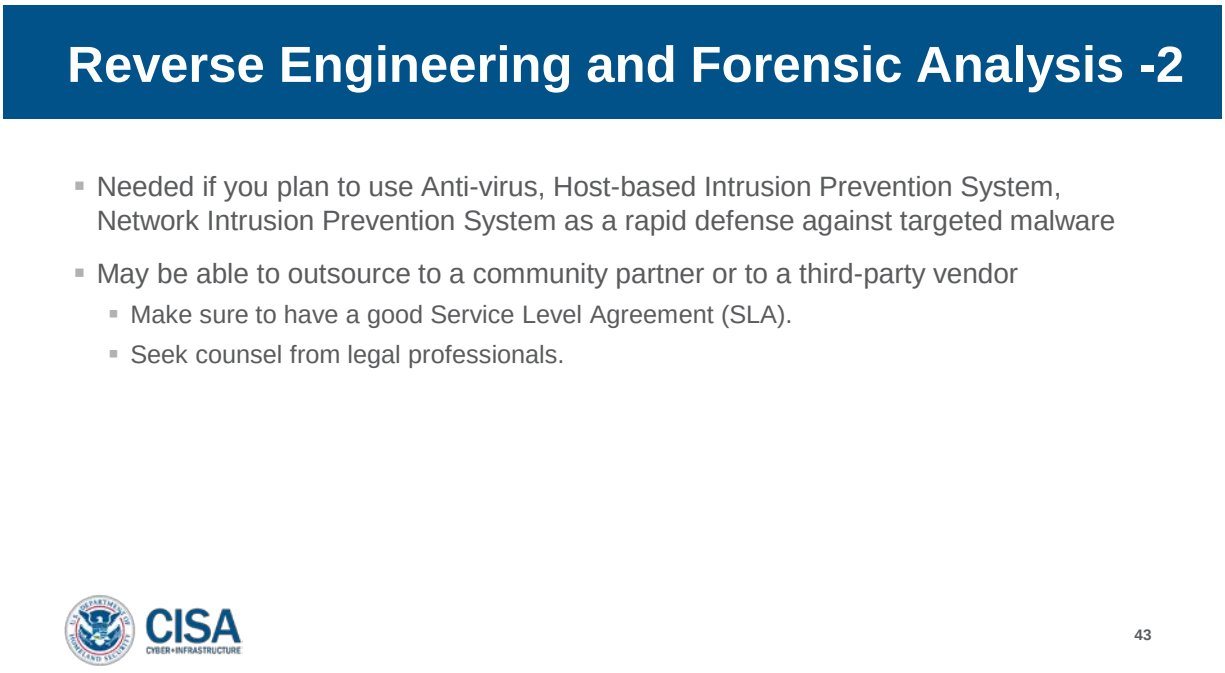
Reverse Engineering and Forensic Analysis -1



**042 Okay. So now you've captured all this forensic data, and trust me, it's not like it looks in the movies. What you really want to do is identify what the purpose of the malware was that you've actually ingested in your system, and what you really want to do is make sure that you can prevent future incidents. Remember, that malware may still be resident on your system, and you need to be able to detect it if at all possible. If the antivirus software that you're using is not updated, you

definitely are taking a risk by continuing your operation, and always be mindful of the fact that you may have zero-day vulnerabilities in your system no matter what. So keep your systems patched and keep looking.

Reverse Engineering and Forensic Analysis -2



**043 Some other things you may want to think about here are the systems that you have online, and you want to make sure that they're patched such that they can have a rapid defense for malware that's already existent and in the wild and it's known about. This is where it helps to have a community of partners that you can tap to understand what they've seen in terms of malware that's infecting their systems, or that they even just identified.

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.

DM18-0098