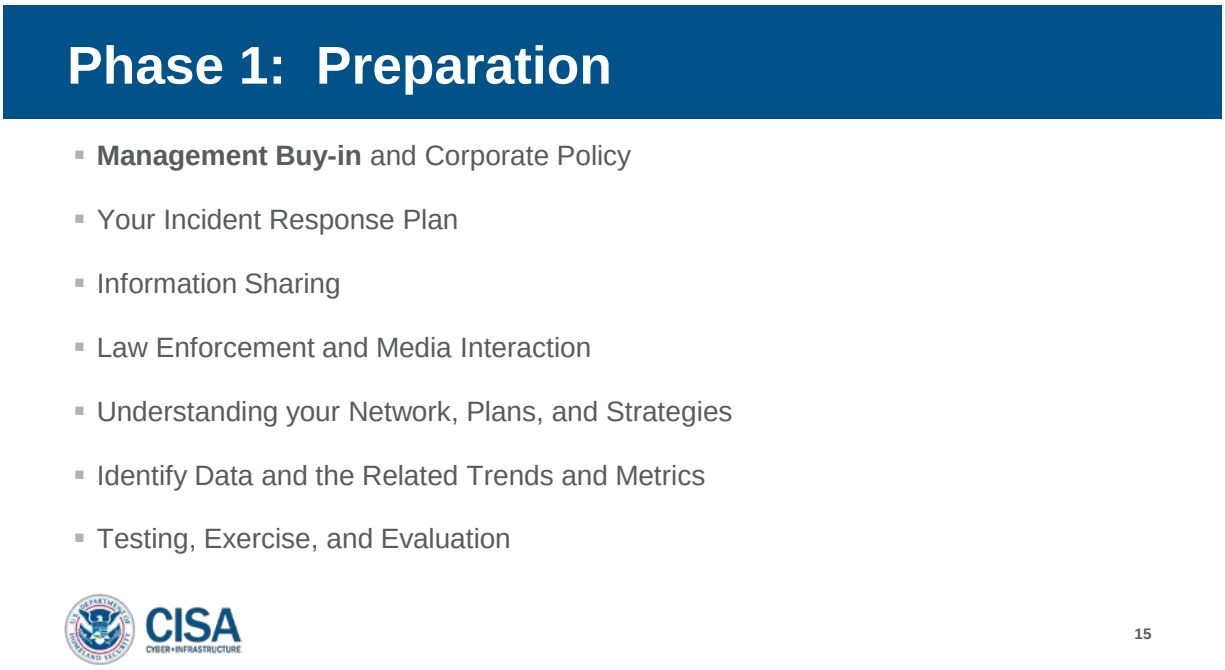
Incident Response Phase 1 of 6 - Preparation

Table of Contents



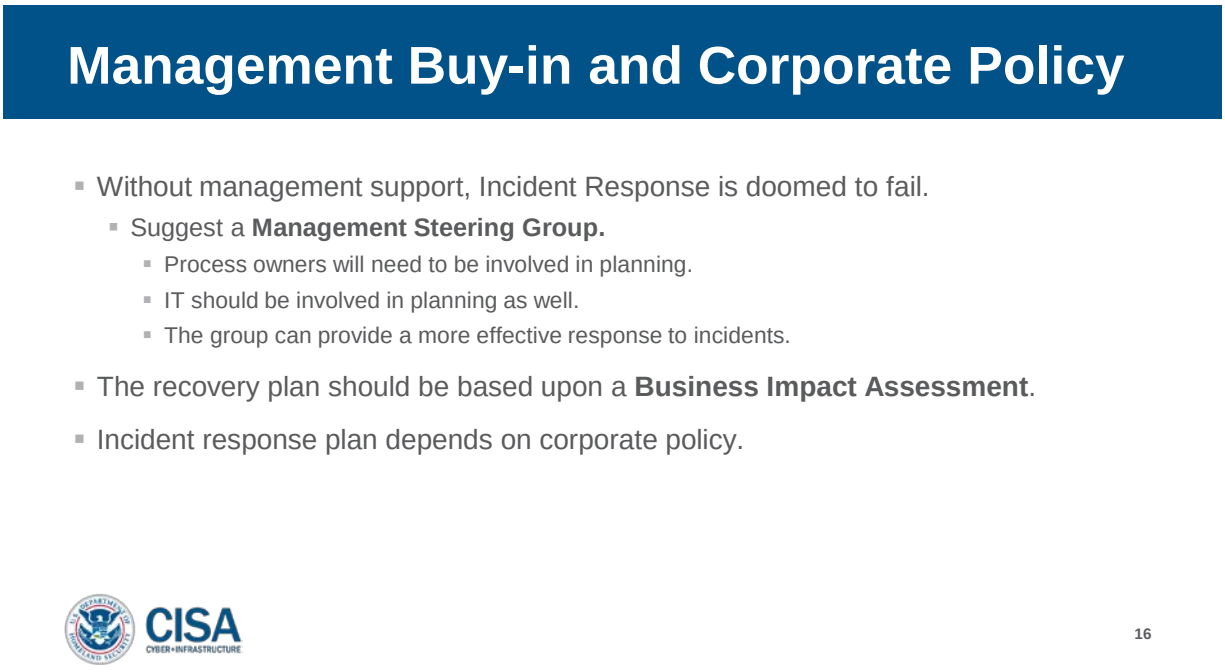
**015 Instructor: So let's talk about these phases of incident response in a little more level of detail here. Remember that phase one was that preparation step. One of the key elements to this step is that you have to have your management team fully backing the activities that you're doing, and you can employ this by having very crisp, corporate policy that ensures that the proper steps are being taken by all people across the organization.

You also have to have a very clean response plan, and when I say clean, what I mean is that it's easily understood and there's as few bugs as possible, few, the fewest points where someone would get to a point of procedure and say, "I don't understand this step." It has to be written in the most base of terms so that anybody could follow it, if at all

possible, or maybe even someone with at least some minimal skills would still be able to understand what's going on.

You have to make sure that information is flowing all across the organization as well. When these incidents happen, sometimes it's just little bits and pieces of evidence that you get from across the organization, and if there's no information flow, you may have a big problem and may not even know it.

Another big key here is to reach outside the organization. You really have to know who you're going to call and how you're going to do it and who is going to be doing that at any given point, especially when you have a major incident that takes place. So as you're going through this, you really need to know too what your critical assets are. What data do I care most about? And you have to also look at, "What data do I have coming into the system and out?" and understand what are the trends related to it? You may do this by putting together some really well-defined metrics so that way you can see those key risk indicators or the fact that you can see that a risk is actually coming to realization, and then ultimately you want to think about, "How is it that I test my people? How is it that I run exercises so I know that my system is working?"

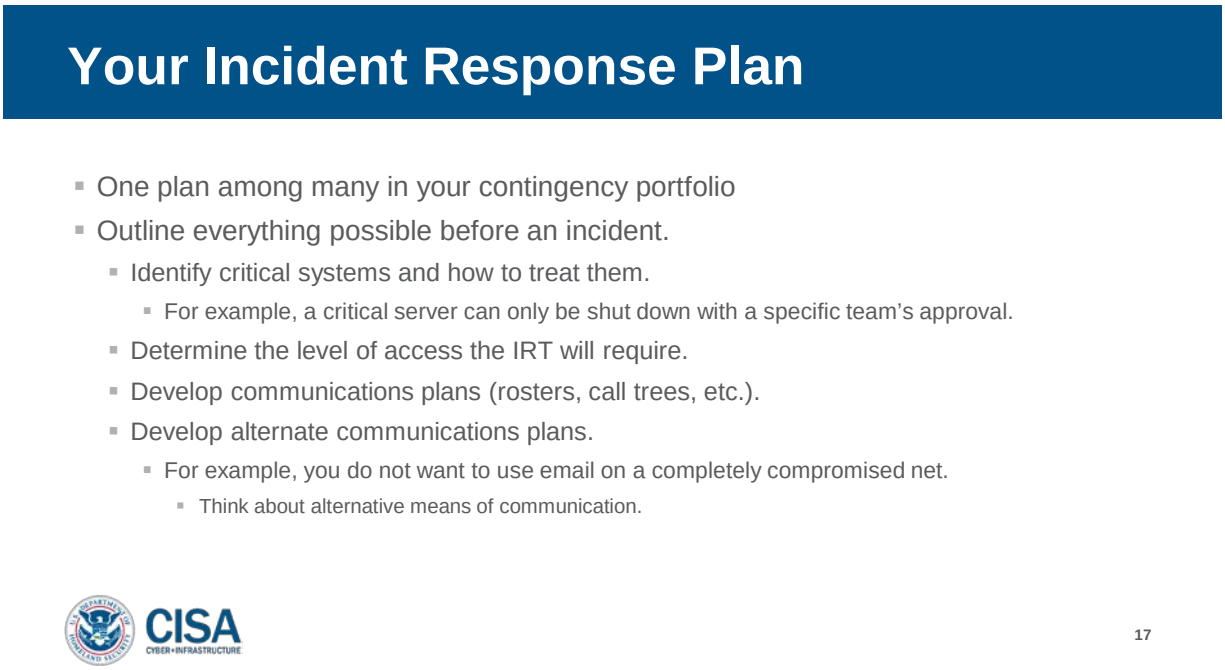


**016 So let's talk a little bit more about that management buy-in piece. One way to approach this is you could establish a management steering group. Imagine a group of executive management team that can get together and actually provide you risk-based decisions. You're going to be bringing them information and they're going to be giving you feedback on what direction to take with your organization and how to make a sharper security team.

Now, what you want to think about here is how you're going to communicate with this management steering group, and the way you're going to do that is largely through business impact analysis. Remember that some of the people on this team may not necessarily understand security like you do. They may not

be the bits and bytes people. Rather, they speak in dollars and cents. So you need to communicate with them in terms of the impacts to the business so that way they can best understand what it is you're trying to convey to them and they can give you the resources you need in return so you can manage your security organization.

Your Incident Response Plan



**017 So you may also be crafting that incident response plan, and there are a couple things to think about here, okay? First of all, you really want to be as thorough as possible. Now, this may be a difficult balance to strike, because if your plan is so dense, if it's hundreds of pages long, there's some people who may just not be willing to pick it up and read it from end to end. So you want to think about how you build it

such that it's easy to read. Policy up front, maybe some procedures, and maybe some tabs to label certain scenario events that you want people to pay attention to.

You also want to look at what level of access that incident response team is going to need to do what they need to do when that actual risk comes to realization. Do they have administrator rights, for example? You also want to make sure that they can communicate freely amongst themselves. You want to make sure that if they need help they can reach out to get other people in the organization or people even external the organization, and you can do this through call lists or trees, however it is you want to attack that. You also want to make sure they have the technology to make those calls as well.

You also want to think about that cold, dark day where you may lose your communication capability. Maybe cell phones are out. So maybe you have to, ah, go Amish, if you will. Take a technology that may be somewhat antiquated in your mind but actually would work well in a situation where all cell phone towers are down. Maybe wireless radio would be an example of something where you could have VHF/UHF communications. That would be a good example.

Information Sharing

- Know your trusted partners.
  - Evaluate how to reach out to them.
  - Think about how they reach out to you.
  - Industry Groups, Trusted Vendors
- Organizations to participate in
  - FIRST (Forum of Incident Response and Security Teams)
    - International memberships (www.first.org)
    - GFIRST (US-CERT) (www.us-cert.gov/GFIRST)
  - **InfraGard** (www.infragard.net)
  - Your City, State, Country CERT

CISA CYBER+INFRASTRUCTURE

18

**018 So on the information sharing piece, first of all, it may not necessarily be that it's just the idea of sharing information within your organization. It may be external as well, with trusted partners that you have. You have to understand how to reach out to them in a sanitary way such that the confidentiality of your information is not violated, especially if you're working with intellectual property.

You really want to think about too how they're going to reach back to you if they're having troubles of if they see something. You can look at industry groups and other vendors maybe within your portfolio of third-party providers that you're using that may be the first best place to start when you're looking for these trusted partners. You can also look at some

industry organizations. I have some listed here. InfraGard's probably your best first bet, and then you want to also look locally what may be available to you.

Law Enforcement

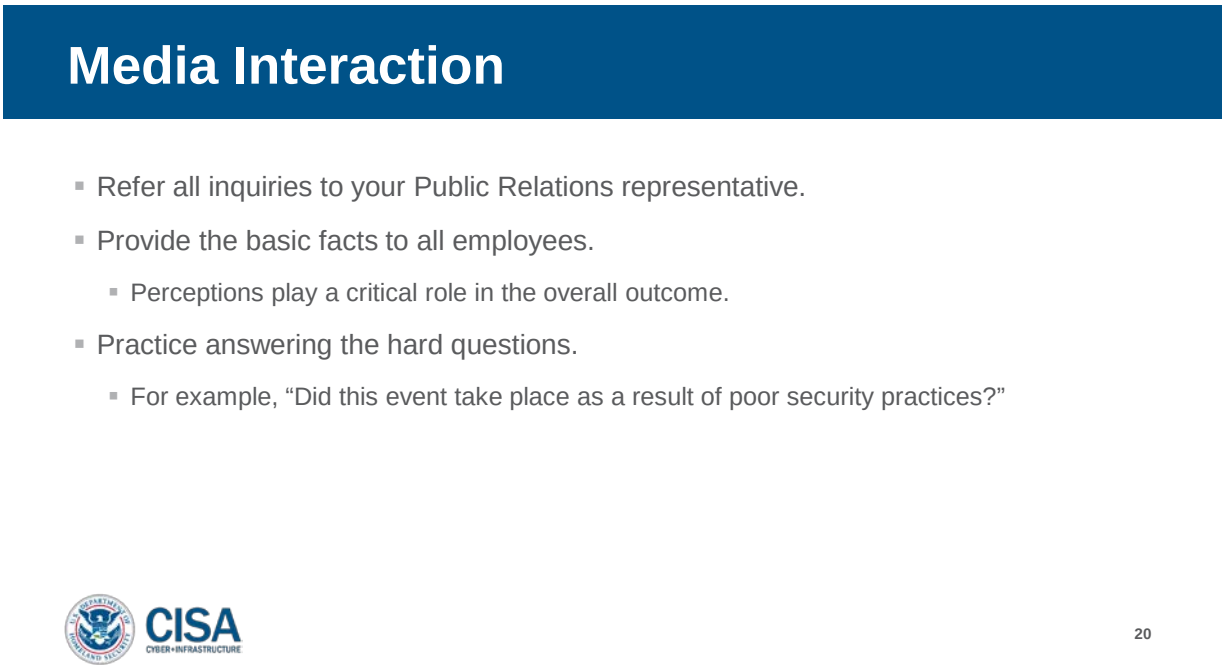
Law Enforcement

- Know who to call before-hand.
  - Incorporate contact information, process for how to communicate, and specify who has authority to call into your response plan.
- Take the initiative to meet your local law enforcement.
  - Learn if they have a cyber crimes division or capability.

CISA CYBER+INFRASTRUCTURE

19

**019 In that regard, local to you may mean law enforcement. You need to know who to call beforehand. Try and hook up with local and federal law enforcement personnel before the incident ever really happens, and you need to have them on your call list.

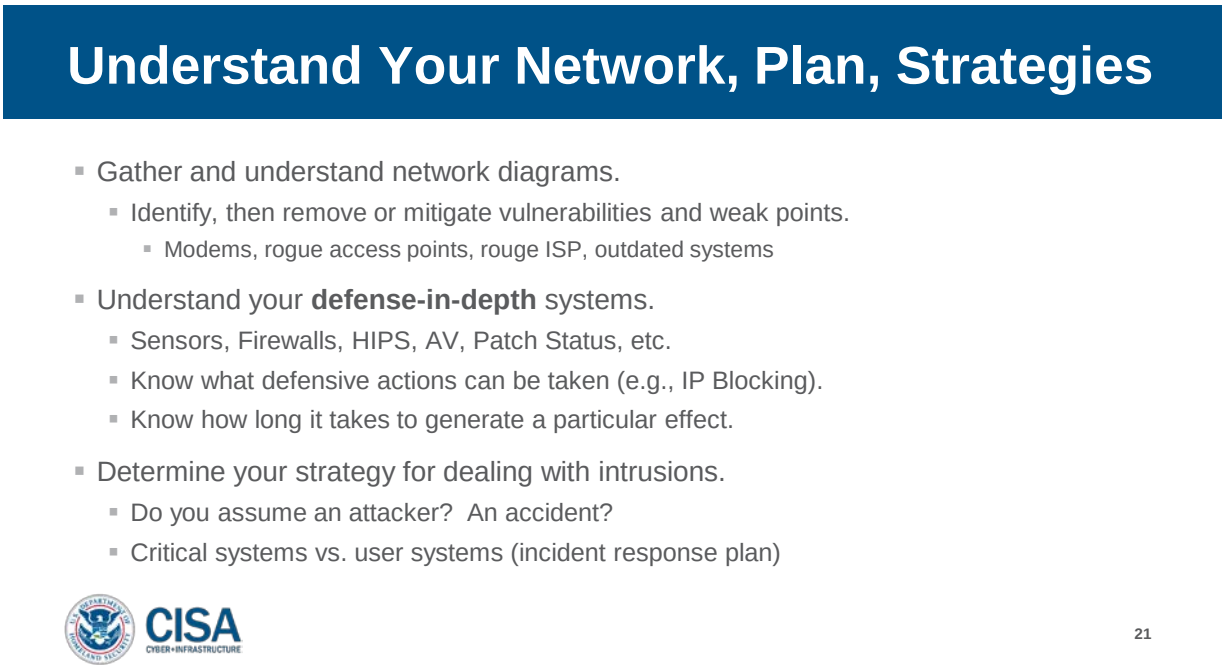


**020 You also need to know how to interface with the media, and this is for multiple reasons. One is you may think that your organization is well informed and that communication is going out. But typically, when events go down, they go down at the wrong time of day. Maybe the dark of night, and the first thing people do in the morning, obviously, is they're going to turn on their TV and they're going to find out that the organization they work for is having major problems. You need to make sure that they're actually getting the information they need so that they understand how to assess what they're seeing in the media. Maybe, for example, you have a universal text list and you send them a quick bit of information that an incident has gone down and they need to be aware that they're going

to be seeing something come up in the news.

The best way to do this is coordinate with your public relations representatives. They're trained to specifically work with the media. They know what to say and how to say it, and they're going to know better if you work with them to establish a plan ahead of time. You really need to think about that cold, dark day and practice and think about, "What are the hard questions that these media people may be asking me?"

I have a good example here, and this one is actually scary if you think about how the heck you'd answer it. "Did this event take place as a result of your poor security practices?" Wow. That is a terrifying way to-- question to get. Think about what that could do to the reputation of your organization if you answer it incorrectly.



**021 It's important to know your assets. You need to understand how your network is built, and you have to understand the strategies around it that exist and that are in place, so that way if an event happens, you can quickly assess where you need to take action. Remember, there's this notion of having a defense-in-depth system. So this is the idea that I have multiple layers of security is set up so that way if something is trying to get through my--to my critical assets, maybe I can see it sooner rather than later, so that way I have enough defense around so that they actually don't get to those assets, and I will limit the negative impact that I have in my organization.

You also want to think about your strategy for actually dealing with an intrusion when it really does happen.

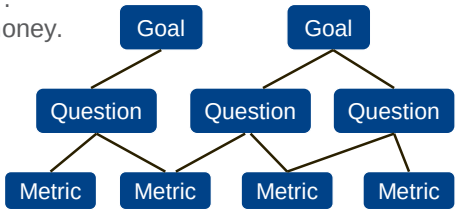
You want to also think about where it might happen in general. This is the understanding of your asset piece again. You want to actually see if you can use pen testing, for example, to understand what an attacker may do in terms of getting to those critical assets.

Trending and Metrics

Trending and Metrics

- Some organizations try to identify all metrics possible.
- **Determine what will give actual insight**.
  - Metrics should have a purpose – and help your IRT.
  - Metrics will have a cost—time, resources, and/or money.

Example Metrics
▪ Bandwidth Utilization
▪ Alert Quantities
▪ Antivirus Statistics
▪ Patch Compliance
▪ Specific Ports Attacked
▪ Infection Location Trends
▪ Help Desk Trends



Use This Process
1. Goal: What is it that you want to know?
2. Question: Define your goal
3. Metric: Answer the question succinctly

CISA CYBER+INFRASTRUCTURE

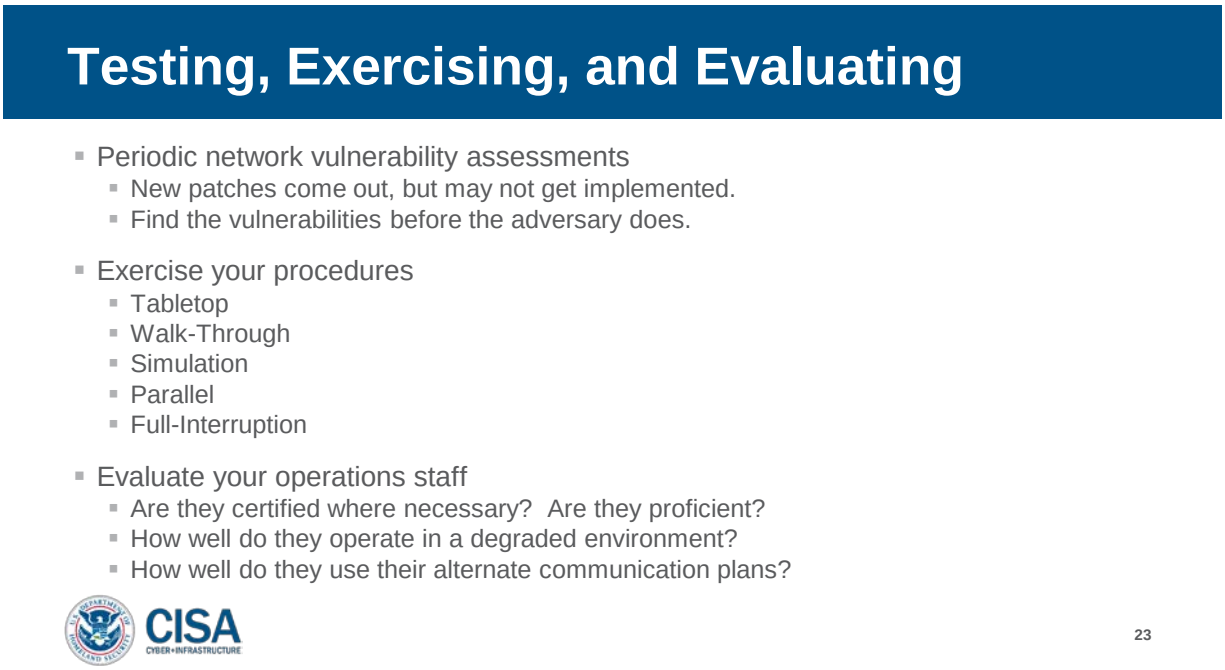
22

**022 Now, what you're going to want to do is also measure what's going on in your organization. You're going to have to establish a set of metrics, so that way that you'll know what your incident response team is looking at to know whether or not a risk is actually becoming realized. Now, the sad part or the hard, difficult part to get over here, is that it actually costs time and resources and money to develop these metrics, and some of them may not even really be all that good. It all depends

on the data that you're getting, and this is the classic adage of garbage in, garbage out. You got to make sure that you're collecting the right data and you're doing it in a manner that will give you that necessary information to affect a good response.

So I have some examples here of some metrics that you may want to consider in your organization. What I would recommend is to use the GQIM model. So you're going to establish goals for your organization and you're going to define those goals by asking questions, and then what you're going to do is establish what indicators may come out of those questions and establish metrics around them.

Testing, Exercising, and Evaluating



**023 So now that you have that picture together, you're going to

actually want to test and exercise your plans and make sure that they actually are operating and doing as you would expect them to. There're different ways to do this. For example, on an easy day what you could do is sit down with your security professionals and go through a tabletop scenario. This is nothing more than a paper exercise, but the good thing is is that you at least know that people know what they're supposed to do, and if they don't, you can give them quick training right there on the spot to make sure that they do understand what their purpose is and what they-- responsibilities they have.

You could also do a walk-through. You actually physically go to their workstation. You walk them through the scenario and see what they're actually going to do, physically. You may even amp it up a little bit and provide simulation.

You could also run a parallel exercise. So this is the notion that I have two separate systems that are mirrors of each other, and I would run the simulation on that mirrored system and understand how people respond to it, so that way I don't interfere with operations. That said, I could also just do a full-blown exercise where I actually do have interruption for my people. These are the ones that are typically the best in terms of getting a high-fidelity understanding of what your people are going to do in terms of incident response, but at the same time, you're going to

understand that you may lose productivity when you do this. You're going to be looking at how proficient your people are responding to these incidents, and you also want to understand that even though the incident happens, how proficient they are at operating an environment where they may not have all the functionality that they used to have, and you may also even take advantage of the idea that you have communication plans in place. Take their cell phones away for a day. Find out how they operate without them.

Notices