Hello. Thank you all for joining us. This is Adam with agility solutions. We still have a few more folks joining us so we'll get started in a moment. We'll be getting started soon. Thank you for your patience.

[ PAUSE ]

Hello. This is Adam Quilty with agility recovery solutions. Thank you for joining us for the top ten most common mistakes during a crisis.

I appreciate everyone's patience.

We're going to go ahead and get started. We will have time for questions at the end, but please do feel free to type those in to the right-hand side of your screen. There's a question and answer bar there that will allow us to keep track of your questions and respond to them as we go.

A couple of housekeeping items first for anyone with hearing impairment who requires computer assisted captions, log in go to Webinar and visit the link that you see on screen there. And that will allow the captioning in a separate window. For everybody else whose joining us, there will be a link
sent to the slides as well as to a recorded version of today's Webinar following the Webinar that will automatically be sent out to you in case you wanted to share the content with anybody who wasn't able to join us for today's session.

Before we get started, I did want to thank preparemybusiness.org and the U.S. Small Business Administration for putting together America's prepareAthon and supporting agility's involvement. If you did want a separate copy of the slide presented during today's session as opposed to waiting for the recorded version that will be sent out to you, you can see the link on screen there. Do be careful as that is case sensitive and you do need to type in the HTTP portion of that link as well as the remainder to have that successfully connect for you.

Without further ado, I wanted to go ahead and get into our content for today. After today's session you should have a better understanding of the common pitfalls for disaster recovery and crisis response, have a better understanding of the implications for downtime from those events for your organization. We're also going to introduce some concepts of resilience that you can dig into further. We're not looking to be the -- cover all of the information or the end all be all in today's session. There's simply too much for us to address. What we are going to do is touch on some of the key points that can then be investigated further for your organization. We're also going to share with you some simple steps you can initiate to help improve and bolster your existing recovery plans. So we will try to make this not only strategic but tactical in terms of some of the things you learn in the takeaways that you can implement.

The ten mistakes specifically that we're going to address today are up on your screen here. We will walk through each in some detail with some examples. Just as a warning, the first couple are the longest. So we are going to keep to today's hour session, including some time at the end for Q&A. But the first couple of points are going to be multi slide and then we'll pick up sleep as we go along.

First and foremost, the most common mistake we tend to see at time of disaster is reliance on a single point of failure. This is a broad statement, but we have a number of different sections here. Reliance on a single point of failure in terms of communications, sympathy recovery site, et cetera. We'll investigate each of these concepts in more detail.

When it comes to communications, looking both at data communications, meaning your networking as well as your voice communications, meaning phones, most of us in our organizations they have a single point of failure. It's more economical to
have a single provider for phones and network as opposed to redundancies in place. But that can cause challenges at time of disaster: If your network topology, for example, is set up in a hub and spoke model where you'd need the centralized network location to be up in running in order for all your second locations, whether those be offices or branches or even people working from home, in order for them to access that network then obviously if that central point goes down, then your entire organization is hampered. Whereas if you take an approach more like MPLS network which has more of a Web model, if you can picture that, you do have the capability of moving network operations from an impacted site to unimpacted so while there is still an issue and disaster response that needs to take place for that impacted site, at least your entire organization isn't down.

When it comes to the voice communications, a lot of folks say, well, we can work from home and everybody has their cellphones. We'll be able to communicate that way. There's a couple of things to think about there. If you do have a single phone carrier, then you still have a single point of failure. If they have towers down or higher traffic, particularly in regional disasters there will be, everybody wants to make a call to their friends and families at once, then you can still be hampered as if you didn't have those phones at all. If you're able to spread out to multiple networks, there's a cost associated with doing that, but the benefit is additional redundancy so you don't ever have all of your employees without communications at once.

Also make sure if you are planning on having folks use laptops and cellphones that they do have additional batteries and chargers for those devices. That is still assuming that the utility power grid is active. It is an additional step that helps you to have those devices actually operational and working in the event of an interruption as opposed to just being a brick you're carrying around with you.

A few other examples here in terms of the single needs of communication, both around e-mail and network connectivity as well as telephony. But again the overarching theme here is having a backup strategy in place so that if your primary goes down you still have a means of communicating within your team.

That is one of the first and foremost lessons learned from all of the recoveries that agility has performed over the years is that even if you don't have a business continuity plan that addresses the specific event that occurs, specific scenario, if you are able to communicate with your team, you'll be able to make decisions and react accordingly and respond to that event in a more effective and agile manner than if everybody's
working in a silo and separate from one another without communication. That really is a key point and a key take away here.

In addition to the communication piece, we often see companies that have a single point of failure in terms of their recovery site. Good on you if you've thought about where your people would go in the event of some type of disaster or crisis. But you do need to think about where that's located and whether that site might be impacted at the same time. If you're using a hot site model where you have a specific address, a building in mind that you would be able to recover to, think about the distance from that site, or rather from your existing site to that backup site and whether it's possible that would it be impacted by the same event.

Similarly, for those organizations that use shared site or shared branching, the idea being let me find other organizations in the area whereby I'll be able to use their space if I'm impacted by a disaster they'll be able to use my space if they're impacted by a disaster. It's a good component as part of a balanced breakfast as it were. It's part of an overall robust business continuity plan. But by itself shared sites and shared branching tend not to be particularly effective because by virtue of the way you're finding those sites they are nearby, they are in the same city, that makes them convenient in the case of an isolated event where only your business is impacted. But it makes it impractical in the case of a larger event.

We have an outage map that shows the counties and areas impacted by extended, over 48 hour, power outages within that impact area. You can see having a planned recovery site nearby simply can't be the end-all be-all. Now, I'm not recommending that everybody on the phone today go out and find a recovery site on the other side of the can you please tree. You can have moderate steps in between. There are other approaches you can take besides only having shared branching as your recovery plan, such as supplementing that with a work from home strategy which has its own strengths and weaknesses. We'll talk more about -- or with other strategies that are available either internally or in the marketplace.

We can also see a single point of failure in terms of key personnel. Really what this amounts to is if there's any one person in your organization who is the only one who knows how to do X critical function, how would your recovery or organization suffer if they were available at the time of disaster. Even the most dedicated employee and worker can have a circumstance where they need to take care of their family or own personal needs first. That could call them away from the
recovery efforts. If you are able to put some cross-training in place and/or simply share the knowledge and resources that they have access to, whether that's a particular software program they manage or files they have access to. Having at least one backup in place can keep you from running into a brick wall when it comes to your recovery.

The third point here on this slide around funding, do be aware that getting back up and running is going to cost some money. If you have a bottleneck or single point of failure in terms of who is able to authorize those funds, that can delay your recovery. If you think of a situation where you lose power and your operations team is locating a generator that they can bring on site and an election to pull that hookup, if they're waiting for the CFO to approve it but the CFO is at home without power and/or outside with a chain Arkansas cutting the tree off of their power lines, your business recovery, or your organization's recovery is going to be delayed until they're able to get those approvals. It can be useful to have an emergency strategy in place. It allows to you bypass some of that red tape at least up to a certain amount of funds.

In terms of single point of failure around power. Power is a common theme we'll be talking about because it is the most common outage or disaster that we see in today's world. As a result many of you on the phone may have planned for an on-site generator or at least generator contracts with local providers, which again, good on you. That's a positive step.

Unfortunately, as in all things with business continuity, there's always more we can be thinking and planning for to continue to increase resilience. My challenge to you would be to think about that on-site generator, whether it could be damaged by the same disaster that knocks out your power. High winds or flooding or anything else along those lines that could damage not only your facility itself but the on-site generator will set you back to square one and looking for an external resource, either an alternate space that you can recover too or another power source.

Even if the generator itself isn't damaged, you want to make sure it's working properly. Following an appropriate maintenance program to help mitigate some of that risk of turning the generator on after six months and finding the fuel has jellified or the pipeline has been compromised.

The example that we see here of the NYU hospital evacuation is extreme but it does bring home the idea that even backup plans such as a generator can themselves fail if not properly tested and maintained.

In terms of the fuel supplies for those generators, we did see this in Sandy and other events as well making sure that you
have either on-site fuel that's stored in a place where it can't be compromised and/or that you have suppliers not just locally but on a regional basis who can bring in that fuel from aspect outside source. We're talking here not only about diesel fuel for the generator that we were just making reference to but also think about your employees. It's all well and good to have the recovery space set up. If your employees aren't able to commute in because they don't have gasoline, again, we're back to square one and only able to work with work from home solution.

So we'll talk more about employee preparedness as we go forward, but that's just something to put a pin in and consider. We can't assume that all of your employees will be ready to report back to work just because you have the recovery setup.

And then in terms of from a people perspective or a training perspective, we talked about cross-training and not having a single point of failure from a skills perspective, but one particular skill I wanted to call out would be publish relations or communicating with the media. Ensure that you have a couple of folks pick out, primary and backup, who are able to speak with the media and then insure all your employees are aware of that so they aren't simply saying no comment or sharing information they shouldn't be but instead directing any media inquiries to the appropriate people.

The way that you control that story examine the presentation of how you're responding to this crisis event or catastrophic event can mean the difference between a public relations nightmare and actually a boon to your business and positive feedback and perception in your constituency or your customer base.

Again, I warned you the first couple are going to be the longest. We will continue to pick up the pace as we continue to go through and address other mistakes. That was all based around the single point of failure concept that we continue to see this as a prevalent mistake across different organizations.

The second point we wanted to address is failure to properly inform our prepare your employees. We talked a little bit about gasoline. But there are a lot of other ways that you can prepare and inform your employees as well.

First off, make sure that they're aware of your business continuity plan, both their part in it and where they can find it and also how it's updated and how it will be shared with them on an on-going basis. So you should have part of your new employee training handbook being referenced to the business continuity plan. Both at the managerial level, those who are looking after other employees and have a part to play, and then also the front line employees who simply will need to know how you're going to be communicating with them in time of disaster.
or where and when to show up after event to help the business to recover.

In addition to the new hires, you want to share that plan on an on-going basis. With everything that people have on their plates in terms of responsibilities day to day, we can't really expect them to remember from one year to the next what their recovery plan is or what their partner recovery plan is. You do need to review that with them at least on an annual basis. Depending on your region, there are obvious times to do that review. If you're in the south eastern United States and particularly prone to hurricanes and tropical storms, go ahead and have this review in the May/June time frame right as hurricane season is starting while everybody is already aware of that threat. Ride that wave of interest.

In terms of preparing employees, the work from home strategy can be a fantastic component to your plan. It tends to be less effective on an on-going basis. For a one-day strategy it may work perfectly fine for you. But the productivity -- you can't expect productivity to suffer from employees used to working in an office if they're working from home for multiple days. Can be technical challenges in terms of accessing software and logging into networks. They may not have the right resources at home in terms of network connectivity and access to consistent reliable power. They may also have their own challenges. If their family members were in the path of the storm or their own home was in the path of the storm they may have other priorities they want to address before they're willing and able to come back to the office.

And then this is further exacerbated if schools are closed and their issues of caring for their children at home at the same time they're supposed to be working. There can be other distractions as well. This all feeds back into why it's important to prepare your employees. We'll talk about a couple of ways to do that to help mitigate the results of that end-all be-all answer of working from home when it's in actuality a little bit more complex than that.

We did talk briefly about cross-training employees. One thing I wanted to add is depending on your business there may be a different response after disaster to what there is before disaster. Obvious example here being insurance, that you can expect to see an influx of claims but perhaps less need or urgency from your producers who are writing new business immediately following an event. Be prepared to prep your staff for longer hours as you're bringing folk in to respond to that event.

When it come to the transportation issues in addition to the fuel we talked about before, there can be shut down of public
transportation. Some of your employees may rely upon that. You can help organize carpools or even make available a block of hotel rooms or other overnight accommodations near the office to make it easier for your employees to report to work. They're helping your business to recover or your organization so it's only right that you be loyal to them and make available whatever resources you can to make it easy for them to address that priority, to help your organization stand back up and in turn be able to serve your own community.

In addition there are some real resources you can point everybody towards you can share with employees, either in a passive way of just making them available or in a very proactive way in terms of organizing seminars and providing benefits who participate in these types of activities, but all focused around helping each individual and their family prepare themselves for disaster. Find out if they have a personal that can help and then organize workshops or seminar or share out checklists to help motivate those employees. Again, make it easy for them to take the steps that you want them to take. There are excellent resources at ready.gov as well as Red Cross focused solely around this personal preparedness. They're freely available checklists and forms that they can fill out to build out these personal preparedness plans.

One you may not be familiar with, do one thing.org really focuses around taking bite size or baby steps to preparedness.

At the end of the course or at the end of the year you'll have a complete recovery or a preparedness strategy as opposed to making it a daunting task where you need to take care of everything at once. I encourage you to share these through your HR or business continuity program in your organization to help make it easier for those employees to be prepared themselves and in turn to help recover your business or organization. The No. 3 mistake we see would be focusing solely on IT recovery. I think all of us know logically there's more outside of IT but there's a couple of points I wanted to make here. first off, in terms of relying too much on outsourced IT that may not be available or have the resources you need when you're relying on them. Comes back to single point of failure. Their own staff may be impacted by this event. Even if they're not, they're going to be serving other customers as well. Their response times during a disaster may be length they happened. There will also be communication gaps in terms of your expectations around time frames and needs, especially when we add in that factor of remote employees or employees working from home. It can be hard enough to get everybody logged in and following appropriate IT policies when everyone's in an office. You can imagine that at the point fold when everybody's
distributed and working from home and in some cases bringing their own device to the network as opposed to their work computer.

So be aware that there may be a gap here. And be aware too even when you have addressed your IT recovery strategy that there are other elements needed as well. It's all well and good that you can access your backed-up data, but you still need other components to make your organization function. You need a place to work, a place where your people to sit. You need computers for them to work on, to access all of that lovely data. All of this needs power and network communications to work.

There are steps you can take to plan for workspace recovery, populating that with furniture and making sure you understand what your power requirements are ahead of time as opposed to scrambling and trying to gather those resources at the time of disaster.

No. 4, properly insure yourself against disaster. I am not an insurance expert. The bulk of what I want to encourage you to do here is consider your existing insurance coverage and talk with your agent about that. I do want to share some common pitfalls in some ways around those though.

So a few ways to mitigate those physical losses we see from particularly weather disasters but other crises as well, you can put in place an asset management program and take accurate inventory so you understand what your potential impact is from a disaster.

And for those assets that are particularly exposed, you can take steps to mitigate those risks or safeguard those assets prior to a predictable event, something that you can see coming. If you're able to raise your computers up off the floor, put sandbags by the door, plywood over the windows and steps along those lines, again, you can mitigate that impact.

There are also some third-party providers that you can notify and postpone or deactivate when you see something coming in terms of turning off your utilities and postponing deliveries and simply making sure that the site is locked down and you have all of the resources you need, whether that's a go kit that you have prepared or critical files that you need to take out of the office before you evacuate.

When you're looking at the insurance policies themselves, be aware of your coverage limits as well as any exclusions. So if you have severe weather insurance but flooding is excluded, be very aware of what that coverage looks like. If you do see that water is seeping in as opposed to being blown in by the wind, your claim may be denied. So be familiar and if there are gaps in your insurance, address those with your agent in
advance as opposed to being stuck with out-of-pocket costs after a disaster.

There is also business interruption or operational downtime insurance that essentially if you can calculate how much money would be lost let's say per hour or day that your organization is not up and running, you can ensure against that loss. So depending on the cause of the outage, you would be reimbursed for the lost business while you're in the process of recovering.

If you have that type of policy in place, your insurance provider may have additional tips and recommendations to share with you. It's in their best interest to make sure that downtime is as short as possible so the claim you're filing is as small as possible.

And then the other policy in addition to the business continuity or interruption would be added expense insurance. That would be for the resources you need in order to get back and up and running to accommodate temporary accommodation force employees or travel living costs for moving them to an alternate site. That catchall is what gives you the funding to actually recover and get back up and lessen that business interruption claim. Those two pieces together work together for you in a disaster recovery situation. Be sure to be familiar with those policies.

One other mistake we would see would be an overreliance on information from third parties. That could be either the utility providers telling you that the power will be back up in an hour even though it's been down for eight hours and thief been saying that consistently. If you can reach out and find information from other businesses in the area or from an election, they may have a better sense of the actual situation on the ground where the line crews are located and the order in which they're coming around. That can help you to make an informed decision about whether you need to bring in an external generator or set up a temporary workspace as opposed to simply waiting out the outage.

If you know that the power is going to be out for two days instead of two hours, you can make appropriate decisions on how to respond to that.

One other thing we would see in large weather events is the fire or engineering Corps who are not allowing you back into the space because it might be compromised. I want to encourage you to respect those experts but at the same time it can help you to get more information and more context if you already know your local officials, meaning the emergency responders, police, fire as well as well as your local county emergency management in advance of an event. If they are part of your conversations
around business continuity and part of your exercises, then that can certainly be helpful in how to work with them most effectively. One of the things you can do in advance to make it easier for them to let you back into your space. Things like insuring that you're shutting off the utilities before you evacuate a building, allow them to know it is, in fact, safe for you to reoccupy that space. That leaves you at the top of the list.

A lot of folks still -- this has changed somewhat since Hurricane Katrina and some of the findings coming out of that event -- but a lot of organizations will still rely on the government, federal or local, to be there to help you to recover. And there are a lot of assets that get put into play and can be provided in terms of assistance in the case of a disaster declaration. But do understand that the priority there may not have your organization at the top of the list or there's an order to the response in that you should expect to -- you are expected, rather, to be self-sufficient for at least 72 hours. So the three-day time frame that you need to have resources for health and human safety first and for most but also in terms of business assistance before you can expect any government resources to be coming in and helping with that recovery.

So the way to accomplish that is really to encourage discussion and planning and culture of preparedness in advance of an event. You simply can't wait until the disaster to develop these relationships and develop these plans. You do need to make sure you're taking those steps to prepare in advance.

We'll talk more about that supply chain point specifically.

No. 6, failure to anticipate the costs of recovery. We've separated this from the insurance piece because it really does go above and beyond. It's one thing to be reimbursed for the out-of-pocket costs, but if you don't have the petty funds or cash available to actually pay those expenses at the time, again your recovery can be delayed or hampered. Cost can be expensive for relocating employees and business functions from your primary space to an alternate space outside of that impact area. You've got the physical travel as well as moving employees families in many cases, childcare, and then paying for remote resources and alternate office space as well as remote network access can all add up.

If you have these relationships in place ahead of time, whether that's through personal and business relationships or through a third-party provider of turnkey office space or through a hotel chain, for example, where you can use their conference center as a crisis management space or recovery
And specifically around the network piece, if you are looking at satellite, whether these are personal satellite phones, which look just like a bigger bulkier cell phone, or we're talking about a satellite dish I for providing connectivity for an office space, that can be a good reliable solution. There is a significant price tag associated with that. You think of how much it costs for these to actually launch a satellite into orbit. They're sharing that cost amongst all their customers. It is going to be more expensive than a landline. If that's the only way to get you connected and your organization back up and running, it may well be worth it. Be aware with that price tag of opportunities for decreasing your bandwidth utilization perhaps by priority advertising critical functions and staff as opposed to trying to get he have been back to work the a once, potentially congesting that network link or other resources.

The best way to have familiarity with all of this is to test. It's to do a dry run and practice in advance. When I say test, we're talking specifically about a hands-on exercise here. We'll talk more about testing as the tenth in today's Webinar, but from a high level, the more hands-on you get, the more assumptions you're challenging and the more findings you're going to have that can help you to fix any challenges or gaps in advance of an actual disaster event.

Other costs to be aware of would be for increased costs or spikes in costs for commodities. Whether that's around fuel, food and water, and other high priority resources. So having petty cash funds available can allow you to overcome that hump while -- I don't like to use the term price gouging, but while those elevated prices are in the marketplace. As demand goes up or supply goes down, your price is going to increase.

And then one last side point that I wanted to highlight, particularly if you do have say a sprinkler system that goes off and damages paper files or there's a fire or smoke damage for of your paper files, there's some excellent document salvage providers out there in the marketplace but they are quite expensive. A lot of expertise and specialized equipment that goes into that. Be aware that recovering paper files can be very pricey. Easily be in the tenths of thousands of dollars for a large project depending on the quantity of documentation. You can help to mitigate some of that by having electronic copies wherever possible or by storing documents securely off-site through an iron mountain or something along those lines, an off-site storage company. So by planning in vice presidents, you can avoid some of those big price tags where you really don't
have another choice. You need to recover those documents. You'll pay whatever you need to but paying a little bit on the front end could have avoided that decision all together.

Coming down to mistake No. 7, failure to properly analyze a supply chain disruption. We want to take a step back at this point in our session from the things that your organization specifically needs to focus on internally and look external stead. We talked already about the bottleneck of third party IT, but what do we do about that? Not necessarily to bring your IT processes in house but some way to understand what planning they have in place and wherever possible have a backup strategy. That may be somebody within your office who's able to do some basic brake fix as a stop gap while you're waiting for that third party IT provider to send resources out and do a full recovery.

The same type of thing in terms of power and communication vendors. There can be a bottleneck there. Not necessarily going to be paying on an on-going basis for a second provider, but having an understanding of those organizations recovery planners themselves will help you better fit into them.

A few other examples that are outside what we typically think of supply chain, meaning physical distributors and the like, payroll companies would be a common one. I'd like you to pro provide your product or service to the marketplace. You need to treat their recovery plan as you would treat your own. Make sure that you have a plan in place that's been tested on a regular basis. The best way to ensure that is include them in your own tests and have those communications on a two-way basis. What are your expectations of them after an event and what's the best way for you to help them be successful. Meaning is there a particular phone number you need to call to report an outage or are there specific steps you can take to follow an alternate process that they'll be following. Maybe that's paper forms at time of disaster. Or a different secure Web site you need to log into in case the primary network fails. If you know those steps in advance you can do what's expected of you at time of disaster, make it easier on that third-party provider to recover effectively and get your systems back up.

Another one we often miss would be your CPA or other attorney -- or attorney rather or other financial firm. Do you have the contact information in place to actually reach them and communicate at time of disaster and have they been involved in your planning and testing processes to understand what's expected of them and how you rely upon them? They may not know they're your critical vendor or take that seriously until you as the customer challenge them to be ready and prepared.

Last but not least looking at traditional supply chain, your delivery and shipping partners understanding what that
protocol is in the event of some type of disruption or interruption. Do you need to be proactive in notifying them to delay pickups and deliveries. Is there a sister company or alternate provider to recommend if their ownership delivery mechanism is disrupted.

And then thinking about what those impacts are. Wherever those impacts are unacceptable, meaning the recovery time frame, cost is too great, you need to mitigate those risks by looking at alternate providers. Whether that's just having an alternate number in your Rolodex or another contract on deck of somebody else you can call upon, you owe it to yourself for all the work you've put into your organization that you don't have a single point of failure outside of your control meaning in your supply chain.

Talked about your employees, now your vendors. Another common mistake would be failure to assess the impact to your customer base. Really looking at it from their perspective. Some of your customers after disaster, particularly long-term outage may not be able or willing to stay with you. Their business needs to continue. How long are they going to wait? If you're one of their critical providers just as we were talking about with up-stream supply chain, now looking at downstream you may be a critical provider and they may have a backup plan or alternate provider in medication if you're down for a particular time frame. Be aware of that. Don't be caught up aware. Have the conversation.

Let them know what you're doing to give them that peace of mind and confidence.

It may not be their choice that they look to another provider but there may be physical restrictions to getting to your site, particularly if you're a bank or credit union or retail organization. If they can't get to your storefront or branch because of either law enforcement or closed roads or curfews that are in place, they're going to need to go elsewhere. One way to mitigate have a presence elsewhere or the ability to set up an ATM, small kiosk at an alternate site. Mobile solutions that agility offers as well as other organizations and other things you can do on your own. They can help you to be less locked into a single positive point that have access restricted to it.

Depending on your business there may be an increase or decline for demand for retail organizations immediately following a disaster there's probably going to be a decline in discretionary spending. But then give it a few days to a week and folks are going to feed to go out and replacing some of the belongings that are lost on that event. For insurance companies the demand is going to go through the roof for
financial institutions. People want to have access to their funds and may be asking to take out new loans and have access to additional funds to help them with repairs. So be aware of the larger context, not just how your organization itself is impacted but what that downstream impact is for your customer base. What time frame you can expect before everything turns back to normal.

Ninth sense would be to properly manage the restoration of operations. This is an entire timeline or process from that initial crush of customers for high demand when the lights come back on and that return to normalcy. We're past the disaster event, response, cleanup and mitigation and starting to get an alternate site back up and now we're to that point where you turned the lights back on the business is back up and running. You need to manage that transition just as you managed the transition from a normal production environment into the disaster or emergency response.

You may have limbed staff because not everyone can report into work. You may have limited access to software and tools. May be working from paper forms for some period of time. Understanding and managing not only internally but with your customers and how those expectations are and how you're going to restore those operations. You can be hampered in terms of though he is communications and setting those expectations if you don't have a way to communicate with the folks who want those updates from you, the stakeholders. You need your Web site to not only be available but accessible remotely and not only by one person but a couple of folks, whether those are internal IT staff or managers and C level folks maybe on the marketing side who have access to those resources so you can communicate and push out messages.

>> Phone calls, if you're not able to answer those calls, make sure you get that number redirected as soon as possible. Even ringing through to an individual cell phone and customizing what that voicemail message is is better than getting a busy or dial tope when somebody calls your number. If they do, the first place they're going is to your Web site to see what's going on. If your Web site's down as well, where are they going next? Someplace else.

So have those steps in place to be able to manage how your customers or how your community and even your vendors and stakeholders are accessing information. If you're using social media, make sure that again you don't have a single point of failure and you've got somebody in charge of that public relations who's able to push out the right message, the right spin to your recovery efforts so it's not focused on the disaster and impact and inconvenience on your response, preparedness and
Once operations are restored, if employees can't or won't repair to work, that's a common issue that we see. It all comes back to the employee preparedness that we talked about earlier. You can still mitigate those out of control by helping prepare your employees in advance and perhaps offering childcare services if you're a larger organization or working together with other businesses, say in your business park or area. We do see some circumstances as well where you're either unimpacted or restored but your supply chain is still disrupted. Whether the traditional supply chain or some of the other organizations like utilities depend, consider. CPA and payroll companies we talked about earlier. Be aware that you may have your doors open and your lights on but still not able to provide those full services or have all employees back to work because of down communications. Make sure you do that proactively so so you don't have customers showing up at the door expecting normal level of service if in fact you're running at 50 percent.

Last but not least before we open things up for questions. The last mistake we wanted to address would be a failure to test your plan. We've really talked about what I hope are a number of pertinent and actionable issues and actions to address in terms of creating a robust business continuity plan. Once you have that in place you really do need to test it. Honestly we here prefer the nomenclature of exercise because it doesn't have that same pass/fail cop notation of a test. Test is a much more recognizable term though. We'll use those interchangeably.

One mistake we see would be failure to even test restoring data. You have backups in place but if those are encrypted and nobody has the password, you won't be able to access it. If they're backed up to media that's sitting right there in the server, you're backing up to tapes that then sit on top of the server cabinet. If there's a fire or other damage to the building, you just lost your backups as well as your primary or production system at the same time that didn't do you any good. Don't just -- do think through it when you're writing plan, but also test it. Understand whether you have access to the backup media, whether you have the expertise to restore, particularly to different hardware if your primary systems were physically impacted, you may need to be recovering to a different system.

And then do you have the right passwords encryption algorithms and software to be able to conduct that recovery. You don't know until you actually walk through that process. Then also see how long it's going to take. Each time that you practice, you're going to get a little bit better, faster, and
uncover new things as well. You don't want to be doing that for the first time in actual disaster event. That's stress nobody needs.

Test your communication. Your alert notification system, whatever means you're using of telling employees we've had a disaster, here's what we're doing it about it, here's what you need to do. Test it. Practice it.

Make sure you can activate it remotely as opposed to only from your work computer. Make sure you can have multiple people, managers sending out messages at the same time so you don't end up with a bottleneck there. And if you're using a more manual system, like calling through a phone list, make sure those numbers are up to date. If the reporting structure is correct so nobody gets left out. You don't want them to be the only person showing up to work when everybody else was informed to go someplace else. And by testing that practicing it, you're also retaping your employees, you're reminding them each time you send that communication out here's what to expect at time of disaster. There's less panic, confusion in an actual event because they remember I need to sit down and wait for a call or I need to check my employee Web site because that's where the updates are shared.

Practice and test the employees knowledge of the plan. If you are the person at your organization with the business continuity hat, whether it's a title or not and you weren't there, do they know what to do? Do they know where the plan is stored and how to reference it? Do they know who else to call? Do they know who's in charge of what?

Make sure that you have a backup in place and you've shared some of that knowledge. Also a good chance to toot your horn, show off everything you've done to prepare and help your organization to be ready. Don't tell management that, just tell them it's all for the good of the business. It can be useful for you as well.

When it comes to supply chain and vendors, include them in your exercises and know their own plans and how those impact you. I didn't mention this specifically earlier but the public organizations are included in your supply chain as well. Rely on your local government and your local emergency management agency particularly at time of disaster. Include them as well, same as your private sector partners. And know your power needs. I mentioned this briefly before. If there's only one thing you would take away from this I would encourage it to have an electrical survey done, whether it's super storm Sandy, other hurricanes, earthquakes, wild fires, and floods. The most common impact is a power outage, the most important step for you to take is to understand what your power requirements are.
If -- at the time of the outage it's going to cause delays, increased cost and you may not be able to get somebody out to take a look at your building because they're too busy with other calls.

So understand what your needs are and then conduct a test exercise whether that's an on-site generator bringing in a temporary generator. Moving to an alternate space or doing an orderly shut down off of your battery backups. Run through that test to make sure that the resources you have in place meet your needs. And if not, go back to the planning board and find an alternate strategy.

I know that was a lot of dense information. I appreciate everybody sticking with us and staying tuned. Again, a recording will be sent out to everybody. Wanted to open things up for a few minutes for questions here. And then for those of you who want to stay on after a couple of questions, we'll quickly walk through a little bit more about the agility solution.

I wanted to turn things over to Nicole Crawford who's also on the line here with us. Nicole, are there any questions at this time that we can answer?

>> Hey, Adam. Yes, we actually had a few questions come in so far. The first person asked if vendors continuity plans are confidential, what kind of info do you think is the most useful to know about their plans.

>> That's a great question. Some of the common questions we see being asked of our customers and they're in turn asking their vendors would be the simple ones, start from do you have a written business continuity plan, when was the last time it was tested and what were the findings from that test exercise? You can delve deeper beyond that if you have particular concerns around pandemic response or around network and intrusion testing or passing a third party audit. Starting from the simple, what did you learn can at least establish that you're on the same page and talking about the same terms.

>> We had another person ask if we had to pick just one place to start based on the ten mistakes you discussed which would be your priority?

>> Obviously they're all my babies and I can't pick just one, but, no, if there's one thing that I would focus on, it would be that single point of failure that we spent a few slides on at the beginning. Because that addresses not only your power requirements that we really emphasize but also the communication piece and ensuring you have things in place so you can make the right decisions at the time of the disaster.

>> Great. We had another person ask, is it normal to have a version of the plan that is published to employees only versus
what management might be able to see?

>> There may be a -- where I tend to see that is if the overall approximates continuity plan, the ones that management and the business continuity team sees is is too extensive, to the point where it's not actionable. So if you have 100 page business continuity plan that's not useful as a handbook for an employee to reference at time of disaster. I would encourage that type of split in terms of a full business continuity plan versus a respond handbook more so than partitioning off the information too much based on business function or management level. Because of some of the points we raised around needing to be cross trained and not having single points of failure in terms of your employees, we want to make sure we don't fall under that same pit fall when it comes to business continuity and partitioning information that might be useful for everybody.

>> We had somebody just write in, would these plans be something that would be expected to be shared with the board and reported as part of the corporate govern naps annual disclosure?

>> Yes, that is typically the case. More and more we see the trend moving in that direction. There are specific industries that have been regulated and have a written business continuity plan with components workspace and network recovery and annual testing for a number of years now. But in the general, both private and public, we do see a telephoned move towards those regulatory requirements and towards an expectation for responsibility on the part of executive leadership and the board for takes those steps towards resilience.

>> We have somebody write in in regards to another local company will allow you to use their space if any problems arise at their facility and vice versa: We were wondering if there's a place the company can place their interest in starting a relationship with another local company.

>> That's a good question. I would start with your local business administration, particularly if you have a focus around spall businesses to share that interest. There may also be ways to network with local organizations, either at an industry conference or users group meeting or something along those lines to express that interest. You can always hit the street and go cold calling, but these relationships tend to be best when they're between two known entities who have some type of partnership and relationship. Just be careful if that's the linchpin of your plan. There are a lot of organizations out there that carry around a lot of dead weight or have twice as much space as they actually need because it's not cost effective. So be realistic with yourself about how much space
or how many resources would actually be available to you if you were to use that shared approach.

>> I think that's it for now, Adam. Thank you.

>> Thank you, Nicole. And thank you to our audience as well. Again, I know it's a lot of information. You do have my e-mail address there on screen. If there are any individual questions that you wanted to ask offline that are particular to your organization. I do want to take a few minutes just to walk through a little bit more about the agility solution. You can always learn more at our Web site as well. But just for some context. Why should you listen to us? What's our experience in terms of these businesses and how did we gather these top ten mistakes? The answer to that is agility has actually been protecting organizations of all types and sizes for over 25 years. We started initially as a division of General Electric to take care of their internal business continuity needs and then really branched out there. Unfortunately our findings have been that most organizations aren't prepared to quickly recover after some type of disaster. They may have plans in place to let them get back up and running in week or two week's time but those haven't necessarily been tested. That time frame may not meet their needs for survivability. Without having some type of real strategy or plan to get back in place and up and running quickly, there's a cascade of effects and impacts. Even if it's just a partial outage, say loss of power to your building, you're loading daily sales, you may have a loss of inventory or certainly reputation and security regardless of with a business you're in. Other outages are no different. Any time you have downtime it causes your customers and your community to question your ability to be there for them in that time of need and that can lose you business and reputation as well as the short-term impact of having closed doors. Having strategy in place becomes the utmost important for being there for your community and employees and really keeping your promise to the business that you built. Agility has a solution in place that is affordable and designed to be scalable for organizations of all shapes and sizes as well. What we've really built is based around these five key elements. We've talked a lot about the planning piece and there is an online planning portal that is available through agility membership. Gives you a template for building a written business continuity plan as well as a place to store all of your plans, whether you write them yourself or through our templates.

In addition there are physical components that help you to recover. The most common need being power. We can provide generators to any of our customers in the case of an agent.
Whether that's powering their existing space or at space that we find for them. No. 3 would be communications, whether that's via satellite or other means that we have within our toolbox. We can provide connectivity to phone and Internet access without relying on any existing infrastructure. Even in a worst-case scenario, some of these big ticket events when we've all got in mind when we think about disaster recovery, we can still give our customers a place to work and a way to reconnect and telephone their business.

The fourth element will be computer systems. Meaning not the software side. We actually don't do that. We're very complementary to data backup solutions, but we don't conflict with any of those. We're simply providing the hardware media that that data would restore to the computers, servers, the working equipment that can be shipped out quickly to get you back up and running right away.

And then last but not least the office space to actually put all of this equipment into. So that if you do have lost or damaged space that we are actually setting you up with a temporary place to work out of, whether that's just used as a command center or whether that's used as office space for your full operations, it has the flexibility to be deployed anywhere and also be to be scalable for any number of staff.

We've been doing this for more than 25 years and we have the infrastructure in place to ensure we're always going to be there for our customers. In fact, we have a 100 percent success rate. Agility has never failed to restore operations for one of our clients at 1/3 time of need. So you can really trust that we would be there for you as well. We've rescued thousands of organizations over the years from big ticket events and isolated events, from single locations to large multinational enterprises. And we are the national leader in the number of recoveries we've conducted, the number of successful recoveries we've conducted and in the quantity of assets delivered in disaster situations. When a disaster happens, when you or one of our customers, within a few hours we would mobilize the resources you into need to get you up and running. Whether that's all of the components we just looked at or just one. We'll work with you to determine what your specific needs are at the time to quickly and cost effectively get all of those resources for you so that business interruption is as short as possible and you and your people and your business are back up and running and taking orders or working with the community as quickly as possible.

The cost at that time of disaster is our out of the pocket costs only. We do not profit from any client's disaster. There's no markup or margin there for agility. You can see
whether you'd heard of agility or not you would have those same needs to get those same resources to get back up and running. If you lose power, you need to go out and find yourself a generator. The difference with agility is we already have the resources in place and the experience and expertise so we can get it done faster, at a lower cost and more effectively. And most importantly we have that 100 percent track record to let you know we will be there every single time. By having the solution in place, we protect our clients, their operations, their reputation and their ability to do business.

I would encourage you to rely on agility. At time of disaster you're going to have a lot on your plate. If you're feeling overwhelmed with the ten mistakes we talked through today and if it felt like a lot of content, I apologize, but it's realistic to all of the complexity that goes into a disaster. Agility is not going to take all of that off of your plate. We can't solve it all for you but we can take off that piece that we are experts at and leave you with far less to worry about so you can do the things that only you can do, like taking care of your employees and communicating with them while agility enables you to have a place to go, a place for them to um can back to work, and the experience to back up that promise.

So we do have more information available at agilityrecovery.com if you'd like to see case studies, watch videos and testimonials, see what an actual recovery looks like and learn more. I would encourage you to do so. I just want to thank everybody once again for taking time out of your busy schedule to learn more about preparedness and to learn more about the top ten mistakes that we've seen so you can avoid some those pit falls yourself. Thank you for taking place in America's prepare Athon and listening to our Webinar today.

Nicole I wanted to open it up one more last time for any additional questions.

>> We did have somebody ask how does your membership apply to a company with multiple locations? They're a legal firm with three offices throughout the Atlantic area.

>> Great question. And for anybody with different outlays and industry we'd be happy to talk with you individually about what we can do for you. The short answer is the solution is cost effective and scalable, not just for single offices but for multiple offices as well. So we can ensure that wherever that impact takes place that we're able to get you the resources to recover that location at a convenient place.

>> Thanks, Adam. I think we're all set for now.

>> All right 679 thanks, Nicole. Once again, thank you all for taking your time. Hope everybody has a happy and safe rest of your day. Take care.