

Disasters Will Happen — Are You Ready?

J. Chris Oberg, Verizon Wireless

Andrew G. Whitt and Robert M. Mills, Verizon VSO

ABSTRACT

This article describes the important considerations and critical steps necessary to develop and maintain a credible disaster response capability based on the experience of a major telecommunication services provider.

INTRODUCTION

Disasters can strike anywhere at any time. Disasters may strike your company or the community you serve. Disasters may be man-made such as the 9/11 attacks or the Madrid transit bombings, or an Nuclear-Biological-Chemical (NBC) attack such as in the Tokyo subway. Disasters may be technological such as the Northeast Power Grid Blackout, or the Minneapolis-St. Paul interstate bridge, or Three-Mile Island. Disasters may be natural phenomenon such as hurricanes (Katrina, Ike, etc.), earthquakes (Haiti, Chile, etc.), tsunami (Malaysia, Samoa, etc.), tornados (Kansas, Mississippi, etc.), floods (Tennessee, New Hampshire, etc.), wildfires or forest fires (Southern France or Southern California, etc.), or even pandemics (1919 Influenza, Avian Flu, Swine Flu, etc.). Disasters may affect hundreds of thousands of people, multiple communities, entire countries, or just one company.

IS YOUR COMPANY READY?

DISASTER PLANNING

There are numerous considerations during disaster planning; a few key elements that must be in your plan include Risk Analysis, Business Impact Analysis, Strategy and Plan Development, and Exercising the Plan.

Risk Analysis — During the assessment of your facilities, consider all risks, internal and external, to each facility itself, to the systems or services it houses, and to the people who work there. The risks to each facility may come from any of the disaster scenarios mentioned above, from the nature of the building itself, the building systems, its location, its neighbors, from the equipment it houses, or simply because humans occupy it. The risks to the systems or services can arise from the facility itself, from physical security threats, from logical security threats, from connectivity issues, hardware or software issues, or simply because humans have access to it. Risks to the people can arise from any disaster

or threat scenario, from injury to fatality, including loss of key personnel needed for business continuity and/or response and recovery efforts. You need to be careful to avoid tunnel vision focusing on the obvious risks and to take an *all hazards* approach.

There are four ways to manage risk. You can accept it, transfer it, eliminate it, or mitigate it. Accepting risk means that you acknowledge the risk, and decide it is sufficiently unlikely to occur or have a significant impact, you need do nothing about it. Transferring risk generally refers to getting insurance to protect yourself against it occurring at all or with sufficient impact to hurt you. Eliminating risk means taking whatever steps are necessary to prevent whatever threat from materializing; actually eliminating risk is highly unlikely, and comes with significant expense. Mitigating risk is to acknowledge that it has some likelihood of occurring, and decide there are acceptable measures to reduce the likelihood of it occurring or reduce the impact to an acceptable level. This is when you prepare and plan for potential disaster scenarios.

Mitigation plans are where backup power plants and generators come from, where diverse circuit routing and network resiliency comes from, where geographic or component redundancy comes from, and where backup tapes or servers come from. Mitigation planning gives rise to hot sites, off-site archives, cross-training people, and exercising your response and recovery capabilities. Mitigation leads to Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), Service Level Agreements (SLAs), and disaster plans. Mitigation is the necessity for Cells On Wheels (COWs) and Cells On Light Trucks (COLTs), Generator On A Truck (GOATs), and Switches On Wheels (SOWs).

Business Impact Analysis — Mitigation comes with significant costs of time, money, and human effort. These costs must be weighed against the potential impact to your business. A good Business Impact Analysis (BIA) must consider all functions your business units perform, and grade them for criticality across several impact categories. For example, see Table 1.

The Business Impact Analysis (BIA) becomes a key tool in gaining your management's acknowledgment of the business risks, and their concurrence and support in mitigation efforts. The resulting criticality ranking will point out the functions that warrant the most attention,

Criticality level	Financial impact of disruption	Stakeholder impact of disruption	Customer impact of disruption	Legal, regulatory impact of disruption	Dependency impact of disruption	Vulnerability level	Time sensitivity
Ranking is for management use to rate functions and focus resources, based on the criticality of the function.	High > \$\$\$/day	High Example: High media attention, high brand impact	High Impacts customer voice/data service	High Significant regulatory or contractual impact	High Numerous critical functions affected	High Single point of failure, Limited recovery capabilities	High Sensitive to interruptions. Function can't afford any down time
Criticality is determined based on the level of impact in the following areas: Financial, Stakeholder, Customer, Regulatory, and Dependencies.	Medium > \$\$/day	Medium Example: Medium media attention, medium brand impact	Medium Impacts customer, for other than voice/data service	Medium Some regulatory or contractual impact	Medium Some functions affected	Medium Recovery sites available, but not immediately	Medium Sensitive to interruptions. Function may be able to afford up to 48 hrs. of down time
Tier 1 functions typically scored High in at least one of these areas. Criticality tier levels for recovery: 1 = Mission critical 2 = Important 3 = Less critical	Low < \$/day	Low Example: Insignificant media attention or brand impact	Low Insignificant customer impact	Low Insignificant regulatory or contractual impact	Low Minimal impact to other functions	Low Auto-failover, geographically diverse, redundant capabilities	Low Less sensitive to interruptions. Function can afford more than 48 hrs. of down time

Table 1. Business impact analysis.

and are most deserving of mitigation efforts, especially when funding is tight. It will also point out those functions that are in need of disaster recovery plans and exercises to test those plans.

Strategy and Plan Development — Armed with the Risk Analysis and the BIA, in conjunction with management's direction and encouragement, you can develop specific strategies for each critical function.

Writing disaster plans can become a line of business by itself, but few companies today have the luxury of allocating high value talent to a dedicated disaster planning effort. More likely, a company will have a small number of individuals responsible for the business continuity portfolio, overseeing the company's preparedness and response program. They, in turn, will rely on the key leaders who own and operate the critical functions performing risk analyses and initial business impact analyses, offering the strategies that can be executed effectively to respond and recover. Senior management will complete the BIAs, and decide which strategy to execute. Senior management must determine who will lead the response and recovery effort.

The military have a saying, "The best plan will not survive first contact with the enemy." That being said, you MUST have a plan. You need to clearly define your goals and state your strategy for achieving them. At the outset of a disaster situation, you will be facing chaos. You will be getting too much information, or conflict-

ing information, or no information at all. You may have damaged facilities, injured employees, or failed systems. A good plan is the cornerstone for everything that follows, a rallying point for your employees, a level set from which response and recovery begins.

So how far down the road do you want to go with developing your plan? A large company will likely have many critical business functions. Do you write a plan for each function and how to deal with each risk that it faces? You could. You might look at all hazards, at all of your risks, and all of your critical functions, deciding they all come down to a handful of circumstances and corresponding recovery strategies. They might include loss of a key facility housing critical functions, loss of the systems supporting critical functions, loss of a third party that provides critical functions, loss of key personnel, or an external disaster that doesn't directly affect you but does significantly impact your community or customers.

Your plan must, at a minimum, include guidelines for plan activation, an immediate incident management structure for the response phase, and initial steps required to identify which strategy will be undertaken. You will need a *tactical* checklist to aid in the execution of your plan when the event occurs. Your plan should include call out lists, notification lists, escalation lists, resources lists, locations information, roles and responsibilities, vendor information, etc. Your plan should identify transition points between

An absolute requirement of any sort of disaster response or recovery plan is communications. You need to be able to communicate with your people to assess their condition, and the scope of the situation you face.

the response phase, the recovery phase, and return to business as usual. Your plan might go further to document everything from choices on how to implement a given strategy, to procedures for recovering a specific system or service, but we don't recommend that.

One important consideration, particularly if you are a technology company and you have technicians that can repair systems and recover services, is when to invoke your disaster response plan? At what point does a problem grow in scope to become a disaster that would activate your response and recovery plan? If it is a large scale disaster with significant damage, with many systems or services down, it would probably be easy to make that determination. But if it is a smaller situation, particularly one that only directly impacts you, when do you stop your technicians from trying to fix whatever it is and turn to executing your emergency plan? At what point does replacement become more cost effective than continued efforts to fix it? That is something your business impact analysis can help you understand, and exercising your response plan can help validate that determination. This is a critical decision your incident commander or incident management team must make.

Another important consideration is maintaining your plan. Your plan should be as tight and concise as you can make it. The more detailed a plan is, the greater the depth that it goes into, and the more maintenance it will require, especially in technology companies. We all know how fast our technology grows, and the speed at which it evolves. If your plan deals with details of the technology your critical functions use, you will have to establish a process for regular review and update of the plan to keep up with the changes. Do not, however, succumb to the temptation of not having detailed procedures on hand because your folks know how to install, operate, and maintain those systems. In a disaster situation, it may not be your regular employees or subject matter experts who are called upon to execute the response and recovery. Those detailed procedures almost certainly exist, are maintained for normal use, and can be included by reference without being part of your plan.

Exercising your Plan — If you don't plan to exercise your plan, don't even write it! If you don't exercise it, how will you know if it includes what you'll need in a disaster situation? Is it up to date? Does it provide adequate direction to your employees and their managers? Does it go into too much detail or not enough? If the most competent and capable people are not available when a disaster occurs, will your company be able to respond and recover? Do your employees have the resources they will need? Does your plan help you to achieve your objectives for response and recovery?

An exercise scenario should be realistic. You can use examples from actual disasters to add a *reality* factor; there are plenty to choose from in newspapers or trade publications.

The key results from an exercise are what you learn from it. What worked? What didn't? What could be done better? Did we spend too much time and energy on one thing and not enough on

another? Did you have the required resources for the tasks at hand? If you could not achieve a particular objective within the desired time, do you need to reconsider that objective, or the resources applied to it? Do you need to reconsider the recovery strategy for that particular function? Do you need to improve training?

Exercises can take a number of forms. You should do a tabletop exercise for familiarization with the plan and processes for the response and recovery phases. You should then progress to a walk-through exercise for hands-on familiarization and training. And then you should have a no-notice exercise, with executive participation, to verify all the pieces fit and work together, recording how close you come to achieving your objectives.

If you have new personnel, personnel borrowed from another department or location, or equipment that is only used for emergency response, you need to train and exercise those resources. If you have back-up media for your critical applications and data, when was the last time you tried bringing that system up using those back-ups? If you have a hot-site, when was the last time you recovered a critical function there? Has it been since you did the rev 4.2 update? If you have automatic fail-over from one location to another or from one machine to another, when was the last time you induced a fault condition to see if the fail-over occurred as expected? Completely rebuilding hardware systems is easy when compared to the thousands of man-hours it would take you to recreate critical applications and data that are critical to your business operations.

COMMUNICATIONS ARE ALWAYS CRITICAL

An absolute requirement of any sort of disaster response or recovery plan is communications. You need to be able to communicate with your people to assess their condition, and the scope of the situation you face. You need to be able to communicate with your suppliers and your customers, with regulatory and government, and your stakeholders. You need to plan for communicating with the media, decide what will be said, and identify who will do the talking.

If nothing else, you need a communications plan. You need to document it, equip for it, and practice it. Everyone, top to bottom in your organization, needs to understand it, understand what is expected of them, understand how to do what is expected of them, and know what their options are if the primary communications they normally rely on cannot be used for whatever reason.

Further, you need to know how to communicate with people and organizations above you and below you in your own company, and in your supply chains.

Further still, you need to be able to do these things quickly. Have those communications paths immediately available; you won't have time to hunt for the pieces and instructions, and assemble them on the fly.

As network service providers, we have all those needs ourselves, and we have our customers looking to us to satisfy those needs for them as well (Table 2).

EMERGENCY OPERATIONS CENTER

There must be some central point where information comes together to be analyzed and presented to those responsible for directing the response and recovery efforts: an Emergency Operations Center (EOC). An EOC function can exist at several levels in a company, and may exist at several levels at the same time in a large company. Where precisely it resides will depend on the scope and severity of the situation. An event affecting a single region might have an EOC operating at that regional level while for an event affecting multiple regions the EOC would likely be at the headquarters (HQ) level. During the 2006 Northeast Power Grid Blackout, our eastern wireless Network Operations Center (NOC) took up the EOC role for the regions affected by the blackout. The western NOC continued normal monitoring of the western US, and took on monitoring of those regions in the eastern US not affected by the blackout.

Your decision makers should be at the EOC. The EOC needs to be scalable to meet the needs of the situation. It may need additional rooms for break-out meetings or for functional area teams.

A key role in EOC operations is a dedicated scribe or recorder to keep a log of activities, and keep track of information or requests coming in and going out. Status reports must be prepared and distributed both up and down the chain of command. Information must be given to other departments, and to other stakeholders, both within the company, and externally. Another key role for the EOC is fielding questions from many quarters so that the people on the ground dealing with the situation are not being interrupted. Yet another will be, at the end of the recovery, to help pull together a comprehensive report of what happened, how it was responded to, the results, and the lessons learned from the entire process.

An EOC will benefit from a tool for collating and presenting information, maintaining current status information, tracking requests and directives, generating reports, and managing trouble tickets. There are a number of such tools available to choose from; several of our units use WebEOC.

Conference calling capabilities are a must. An EOC, whether at a HQ or an area or regional level, should have its own conferencing capability. Our NOCs maintain multiple dedicated conference bridges for normal use, and for EOC emergency use. In any given response situation, there will be several bridges in use simultaneously. A typical set up for a large regional scale response effort might see one bridge in use for the field technicians and their managers, another for the vendors supporting the response, another for the switch techs and their managers, and another set aside for management reporting and updates. Either the NOC or the controlling EOC will have the conference bridges up on speakers to monitor activity and jump in if necessary. Having your own conference bridges is strongly recommended, both for privacy and because commercially available bridges can become saturated in a large-scale event.

Traditional wireline (PSTN) telephone service	Data
Wireless telephone service	Email
Cable telephony	Instant messaging
Satellite telephony	Facsimile
Two-way radio	Video
Pagers	Telemetry
VOIP	SCADA (supervisory control and data acquisition) systems
Broadband Internet (wired or wireless)	Couriers
Broadcast TV and radio	

Table 2. *How to communicate?*

Toll-free numbers are fine for business as usual activities. If there is a vendor (or anyone or anything else) that you must be able to reach in an emergency, make certain that you have the real 10-digit telephone number that will get to them. Toll-free calling may not work in an emergency because of congestion in the networks or damage to the networks. Similarly, if you have toll-free numbers for people to reach you, make sure that the people that you want to hear from have a real 10-digit number for you.

International dialing may or may not be something you do routinely, and your phone system or phone service may not be programmed to allow it. If you plan to use satellite phones for bypassing the terrestrial network to reach an isolated location, it may be necessary for you to have international dialing so that you can call those phones. If you get tech support from a vendor overseas, but you normally call a gateway number in the US which routes you to them, you may need to have international dialing to be able to reach them. All these things you need to know and plan for and equip for and practice before something happens.

MONEY MATTERS

If your disaster includes widespread power and telephone service outages, you (and your employees) will probably find out pretty quickly that the banks are not working, nor are their ATMs. If you use company credit cards for small purchases, you are likely to find that credit card validation systems at retail locations are not working, nor for that matter are the retailers' cash register systems likely to be working. Where, and how, are you going to obtain and pay for fuel for your technicians' vehicles? If the outages persist, how are you going to pay your employees? How are they going to pay for the things their families need? Don't lose sight of that issue; you won't get far without your employees.

You will want to keep track of your disaster response expenditures. You may find yourself

Agriculture/food	Emergency services
Banking and finance	Government facilities
Chemical	Healthcare and public health
Commercial facilities	Information technology
Critical manufacturing	National monuments and icons
Dams	Nuclear reactors, materials, and waste
Defense industrial base	Telecommunications
Energy (except nuclear power)	Postal and shipping
Transportation systems	Water

Table 3. *Critical infrastructures.*

paying for repairs to your buildings, buying a lot of fuel for generators, buying replacement hardware, ordering new circuits, hiring clean-up workers, paying a lot of overtime to your employees, etc. You may have to arrange transport for employees with copies of your applications and data to a distant hot site, and you may have to pick up their expenses at that location for quite some time. You should ask your accounting people to establish particular accounts for all this well in advance of any disaster events, and to work out with them how that will actually be done in the throes of a disaster response.

Talk to your insurers. Insurance is all about risk, and good insurance companies will have risk management programs that can help with risk analysis, and business impact analysis and recovery. They don't want a disaster to happen to you anymore than you do, and will want to see you come back quickly and strongly. If you do suffer significant damages, make sure to do accurate damage assessments (pictures or video will be very helpful), and to track repair or replacement costs, labor costs, etc. Even big firms with high deductibles in their coverage can find themselves overrunning their deductibles in a hurry in a major disaster.

PERSONNEL MATTERS

No response or recovery effort is going to succeed without people than can apply the necessary skills, resources, and energies to solving the problems. Your people are themselves a key resource, and must be cared for physically and psychologically.

From the very beginning of a major disaster situation, you will need to account for your people in the affected area, determine their locations and the condition of those locations, and determine their condition and that of those around them including their families. If an employee is worried about their own health and well-being, or that of their family, they are not going to be entirely effective in helping with your response efforts.

In Haiti, we saw the local wireless companies setting up tent camps on their own properties to provide shelter, food, water, and security for

their employees' families so that their employees could go out and work on recovering their networks.

Early in a disaster situation, management will need to assess the situation, the damages incurred, and the resources available for response and recovery. The personnel situation needs to be part of the consideration. Do you have the right people available to respond with, and are those people actually available? How long is the response going to take? Do you need reinforcements in any particular skills or areas? Where do those reinforcements come from? How do they get to where they're needed? How do you care for their needs once they get there? Can you work around the clock or only during daylight hours? How do you care for anyone who may be injured in the effort? Are you bringing in vendor personnel to assist? Answer all the same questions for them, too. Not just the workers, but managers too. Not just the folks out in the field, but also the supporting personnel in the engineering offices and the operations centers.

You will need to make it clear to all concerned from the outset what your expectations with regard to personnel issues are. Your employees need to know what you expect of them, and their managers, in terms of care for their own safety and security, and job performance. You will get their best efforts if you and your managers make your best efforts to watch out for them.

THE ROLE OF GOVERNMENT

In any major disaster, government entities at the federal, state, and/or local levels will play an important role. Your response leaders should be trained in the National Incident Management System (NIMS) so that they can understand and effectively communicate with government emergency managers.

The US Government's National Response Framework (NRF) defines what it refers to as Critical Infrastructures (CI), which are essential to the survival of the country (Table 3). Most of the key resources of the CIs belong to the private sector. Each of the CI sectors has an Information Sharing & Analysis Center (ISAC) where government and industry can come together to share information on preparedness and response issues. Links to information on the CIs, the ESFs, and ISACs can all be found on the Department of Homeland Security (DHS) web site.

The NRF also describes Emergency Support Functions (ESFs) which must be maintained in order for the country to respond to and recover from a disaster (Table 4). The private sector is a key player in emergency response and recovery, and works alongside government in each of the ESFs.

Communications is recognized in the US Government's National Response Framework (NRF) as a Critical Infrastructure (CI), and as one of the 15 key Emergency Support Functions (ESFs). All of the other CIs and ESFs rely on communications in order to do their part in a disaster response and recovery.

Governments will have their own communica-

Emergency support functions	Federal sponsor agencies
ESF #1 – Transportation	Dept. of Transportation
ESF #2 – Communications	DHS (National Communications System)
ESF #3 – Public works and engineering	Dept. of Defense (Corps. of Engineers)
ESF #4 – Firefighting	Dept. of Agriculture (U.S. Forest Service)
ESF #5 – Emergency management	DHS (FEMA)
ESF #6 – Mass care, emergency assistance, housing, and human services	DHS (FEMA)
ESF #7 – Logistics management and resource support	General Services Administration and DHS (FEMA)
ESF #8 – Public health and medical services	Dept. of Health & Human Services
ESF #9 – Search and rescue	DHS (FEMA)
ESF #10 – Oil and hazardous materials response	Environmental Protection Agency
ESF #11 – Agriculture and natural resources	Dept. of Agriculture
ESF #12 – Energy	Dept. of Energy
ESF #13 – Public safety and security	Dept. of Justice
ESF #14 – Long-term community recovery	DHS (FEMA)
ESF #15 – External affairs	DHS

Table 4. *Emergency support functions (and their federal sponsor agencies).*

tions networks, but almost all of that relies upon systems and facilities provided by the private sector. To a large extent, the private sector also provides the interconnection and interoperability between those networks. The priority services that governments depend on for their communications in a disaster are largely provided by the private sector. Governments will rely heavily on the private sector to restore communications in the wake of a disaster.

In a disaster response, the private sector must depend on its own plans and its own resources. The only major things we ask the government for in an emergency are “Access, Fuel, and Security”.

In an emergency, police (and perhaps military personnel) will control access to the affected area. If we are to assess any damage to our systems and services, we need to be able to get in and inspect them. There is not, in the US, a standard for access control that is recognized by law enforcement at all levels. Each US state is responsible for establishing those rules within its own boundaries, and even then authorities at the county or city level may take it upon themselves to establish their own criteria. Numerous schemes have been put forward by governments at different levels and by the private sector, but none are universally recognized. But we as communications providers nationwide must be able to get access, and are thus forced to work out recognition and access processes with each jurisdiction we serve.

Fuel is certainly a necessity at many levels of a response situation. Relief centers, hospitals, emergency operations centers, airports, helicopters, fire trucks, power crews, and so on, all need fuel. All communications systems need power. Our core network systems typically run on –48 VDC, and we typically have sizable backup battery plants to support them. And those will be backed up with large generators that need large amounts of fuel. A major switching center will have one or more generators on the order of 1000 KVA, and fuel for 48–72 hours to support the systems and their cooling plants. As the systems fan outward toward the edges of the network, you find less equipment, but more of it in more locations, and all of that requires power. Battery plants and generators, albeit smaller, will still be found, and again they will need fuel. The circuits connecting the edge of the network to the core will route through equipment that needs power. And right at the edge, the customers’ devices will require power whether it’s for a network interface device or for the terminal equipment. Battery powered laptops and wireless phones will need to be charged. Our technicians will be relying on their vehicles to get around to all these locations to repair or replace equipment to restore service, and they need fuel. Getting fuel to all these locations, as well as to all the other sectors that need it, becomes a major effort which government can assist with. If fuel supplies are not adequate to the demand, then government can step in to prioritize distribution and delivery.

We'll conclude with the three components that you must have to succeed in a response and recovery situation: a well thought out and exercised recovery plan; a well thought out and exercised communications plan; and strong, competent, adaptable incident command leadership.

Security becomes an ever greater concern as the impact of a disaster becomes broader, and the duration of a state of emergency becomes longer. Security must be provided for medical supplies and personnel, and delivery of medical services, for supplies of food and water, and their delivery to where they're needed. Security must be provided to locations providing essential services, and to those engaged in delivering those services. In a major disaster situation, the whole of the affected population, and particularly all those involved in the response and recovery efforts, must have a sense of security so that they can do what needs to be done. This is clearly a key role for government.

There are some other things that government can do to help. The US Government, collectively, is a very big customer of the telecommunications industry. A couple of the tools we have developed for them have been made available for broader use in emergencies. These include Telecommunications Service Priority (TSP), Government Emergency Telecommunications System (GETS), and Wireless Priority Service (WPS). The government is currently pursuing initiatives aimed at extending those capabilities into Next Generation Networks. Industry and government need to continue to work together to make that happen.

The government also provides a vast amount of information on emergency preparedness and response, for private citizens, for businesses, and for government entities. The FEMA and DHS websites include links to this type of information. Many other government agencies also have disaster information on their web sites particular to their areas of responsibility.

CONCLUSION

Within the bounds of this article, we cannot itemize or describe all aspects of a disaster response or recovery plan. It is our intent to share with you our real-world experience, and to raise issues that are critical for you to consider as you develop your plan. A disaster can be com-

pared to a "come as you are" party. When it begins, you can only bring whatever you have immediately at hand.

We'll conclude with the three components that you must have to succeed in a response and recovery situation:

- A well thought out and exercised recovery plan
- A well thought out and exercised communications plan
- Strong, competent, adaptable incident command leadership

BIOGRAPHIES

J. CHRIS OBERG (Chris.Oberg@VerizonWireless.com) is a 20-year veteran of the U.S. Army Signal Corps and the White House Communications Agency, and a 20-year veteran of the wireless industry with Bell Atlantic Mobile and Verizon Wireless. He has served in installation, operations, maintenance, administration, compliance, and planning roles in both careers. He is currently responsible for network emergency preparedness, risk management, and physical security, and represents Verizon Wireless in various industry and government fora.

ANDREW G. WHITT has over 32 years experience in the telecommunications industry, most of that time serving in a technical or operational support capacity. As head of Verizon Wireline's National Switching organization, his responsibilities includes overall switching network reliability, service impacting event management, and catastrophic outage response/restoration. Disaster recovery experiences include recovery from floods, tornados, hurricanes, 9/11 terrorist attack, and various other larger scale outage events. He is the current chairman of National Electronic Services Assistance Center (NESAC), a North American technical support leadership forum associated with QuEST Forum.

ROBERT M. MILLS has held various engineering and operations positions within in the telecommunications industry over 27 years. He began his career with New York Telephone/NYNEX in Buffalo, New York, as a network engineer. He then moved to MCI Communications into a network operations role. He rose through the ranks to director, and he is now a member of Verizon. He held the position of Global Transport and Switching NOC director for over 10 years being responsible for one of the world's largest transport networks in over 140 countries across the globe. He holds a B.S. degree in electronics engineering from the Ohio Institute of Technology and an M.S. degree in telecommunications and computing management from Polytechnic University, New York.