Hurricane Andrew (August 1992): Organizational Issues

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University, Northfield VT

In the preceding articles in this column, I introduced some of the events of the great storm of 1992 that swept through the Caribbean and part of the south-eastern United States and reviewed some of the valuable lessons learned at that time and how they have improved emergency response in the decades since the early 1990s. Today, I'll continue with insights from the Master's of Public Administration program< http://mpa.norwich.edu > at Norwich University< http://www.norwich.edu > in Vermont, which includes two courses that bring students into detailed discussions of today's standards.

The second of the two courses in the MPA concentration in Continuity of Government Operations is BC521, "Incident Management and Emergency Response."

In developing a response plan, you can't plan for what you don't understand. And you can't expect to wait until you are perfect to have a plan! Critical path analysis< http://www.mindtools.com/critpath.html > tells you what absolutely has to be done first and what gets done second and third. The critical path lays out which tasks depend on completing other priorities first. Politics has nothing to do with it: putting something first has to reflect absolute need and dependencies, not feelings of personal worth.

Similarly, continuous process improvement< http://www.processexcellencenetwork.com/process-management/ > , which is at the core of many US military organizational policies< http://www.armyobt.army.mil/about-continuous-process-improvement.html > defines *thinking* about how we work as a priority for everyone. One of the most frustrating responses anyone can receive in an organization after questioning why a procedure is in place is "Well, we've always done it that way." Every aspect of our work should be subject to rational thought, re-evaluation and improvement – and without having to worry that anyone is going to feel personally attacked when the someone raises possibilities for improvement, particularly in designing and refining incident response processes (IRP), business continuity plans (BCP), and disaster recovery plans (DRP). We must practice egoless work< http://www.mekabay.com/nwss/435_egoless_work.pdf > as defined in Gerald Weinberg's famous text,

The organizational position of a person has nothing to do with the possibility of useful contributions for improvement; indeed those with hands-on, direct responsibility for accomplishing specific tasks may have more insight into what works and what doesn't work than managers at increasing degrees of remove from day-to-day operations.

Emergency Operations Centres (EOCs) are also called *command centres*, *situation rooms*, *war rooms*, and *crisis management centres*. These buildings, sections, or portable locations are where people can coordinate all the responses required to ensure smooth, effective delivery of appropriate responses to all aspects of an emergency. Fixed-position EOCs have to be built to withstand an appropriate level of stress (which should be predicated on historical information about types of stress particular to a given location, such as earthquakes, floods, tornadoes, hurricanes and so on). It's no good having an EOC that blows away in a high wind – whether it's a permanent building or a mobile EOC constructed inside, say, a reinforced trailer that can be transported to an appropriate site using an 18-wheel tractor-trailer rig. Such mobile EOCs will be equipped with their own portable electric generators, mobile communications centres, and even pneumatic outriggers to stabilize the structures against high winds or post-earthquake temblors.< http://www.directionsmag.com/articles/the-next-generation-emergency-operations-center-and-other-carnegie-mel/204433 >

The EOC will also depend on an Incident Command System< http://www.fema.gov/emergency/nims/IncidentCommandSystem.shtm > (ICS) that integrates computers, wireless and cabled networks, radio and mobile phones into a unitary system for effective management of operations. The EOC must help coordinate daily operational activities, including immediate communication between the EOC staff and personnel on the ground. Communications are central to success in all emergencies. Emergency radio systems are already in use by police and emergency response teams; remember that landline phones and often mobile phones may be severely disrupted in national disasters. An Event Information Tracking< http://www.davislogic.com/EOC.htm#Event > (EIT) system provides audit trails to track all communications; these records give us the data we need for after-incident analysis, an essential part of continuous process improvement.

During the development of all IRP, BCP and DRP, practice is essential. These response plans are so complex that no one can predict which parts will work and which will fail. Using simulations< http://www.depiction.com/webinars/lanl > can be helpful, but there's no substitute for practicing the actual operations (e.g., on a weekend) and recording as much as possible about the events using audio and video for post-mortem analysis. The US Federal Emergency Management Agency (FEMA) has suggestions< https://hseep.dhs.gov/pages/1001_HSEEP7.aspx > for structuring such exercises.

Be aware that although trained first responders will be an essential and much-valued part of the plan, you will inevitably find volunteers – sometimes even from other countries – flying and driving in to help. Be prepared to use them wisely: the emergency is no time to have to stop and figure out what to do with these resources.

As for planning for your own agency's continued operations, you need backups of your data and your software that are kept away from the site you are protecting. You should think about storing such data in a different region from the area that could be affected by an emergency such as Hurricane Andrew. Some recovery sites are hundreds of miles away from the protected agencies.

You will have to think about what type of recovery site< http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/4/html/Introduction_To_System_Administration/s2-disaster-recovery-sites.html > you need: cold sites are cheaper, but they take longer to get up and running. In contrast, hot sites may actually be usable for normal processing. The stock exchanges, for example, use all the computers in both their normal and their hot sites for processing – but each part can handle the full load without difficulty in case of emergency.

Where will people work if your main offices are inaccessible? Finding places for office workers is tricky. If you can afford to build spare work areas, great – but you may have to settle for searching out – in advance – alternate sites that will still support the level of electricity use, water, and communications you need. As for sharing resources with separate agencies, it's tough to implement. Even if you can share hardware and software, how are you going to fit two offices of people into a single office if both are heavily used at all times? Can you work split shifts? If not, you're going to get into trouble.

Readers may wish to download and use "Supplement: Lessons from Hurricane Andrew" which is available as a narrated< http://www.mekabay.com/courses/academic/norwich/is342/is342_lectures/csh5_ch57-58_bcp-drp_supplement_andrew.pptx > PowerPoint file.

For additional readings, see

- CDC "Emergency Preparedness & Response."< http://www.bt.cdc.gov/ >
- DISA (2004). "Computer Incident Response Team Management CD-ROM."< http://www.mekabay.com/infosecmgmt/disa_cirtm_cdrom.zip >
- DHS "Critical Infrastructure."< http://www.dhs.gov/files/programs/gc_1189168948944.shtm >
- FEMA "Are You Ready?"< http://www.fema.gov/areyouready/ >
- FEMA "Emergency Management Guide for Business & Industry."< http://www.fema.gov/business/guide/index.shtm >
- FEMA "National Response Framework Resource Center."" http://www.fema.gov/emergency/nrf/ >
- Kabay, M. E. (2011). "Backup." Lecture notes PPTX< http://www.mekabay.com/courses/academic/norwich/is342/is342_lectures/csh5_ch57_backups.pptx > & PDF< http://www.mekabay.com/courses/academic/norwich/is342/is342_lectures/csh5_ch57_backups.pdf >
- Kabay, M. E. (2011). "Business Continuity Planning." Lecture notes PPTX< http://www.mekabay.com/courses/academic/norwich/is342/is342_lectures/csh5_ch58_bcp.pptx > & PDF< http://www.mekabay.com/courses/academic/norwich/is342/is342_lectures/csh5_ch58_bcp.pdf >
- Kabay, M. E. (2011). "Computer Security Incident Response Team Management." Lecture notes< http://www.mekabay.com/courses/academic/norwich/is342/is342_lectures/csh5_ch56_csirts.pptx > &< http://www.mekabay.com/courses/academic/norwich/is342/is342_lectures/csh5_ch56_csirts.pdf >
- MIT WORLD "Emergency Response" topics< http://mitworld.mit.edu/searches?term=emergency+response >
- MIT WORLD "Disaster Recovery" topics< http://mitworld.mit.edu/searches?term=disaster+recovery >
- Ready.gov< http://www.ready.gov/ >
- Weinberg, G. M. (1971). *The Psychology of Computer Programming.* Van Nostrand Reinhold (ISBN 0-442-29264-3). Xv + 288. Index. Still in print: Silver Anniversary Edition (1998)< http://www.amazon.com/Psychology-Computer-Programming-Silver-Anniversary/dp/0932633420 >. See pp 52-60 in particular about egoless programming.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >