

# Hurricane Andrew (August 1992): Lessons Learned

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

*In the preceding article 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. Today I'll review some of the valuable lessons learned at that time and how they have improved emergency response in the decades since the early 1990s.*

In the wake of the demolition of thousands of homes, a surprising issue cropped up: insurance. As attorney Gary A. Poliakoff, JD explained in his 2004 article, "Lessons of Andrew and Iniki: Adequate insurance and document safety are just two of the lessons emerging from Hurricanes Andrew and Iniki." < [http://www.becker-poliakoff.com/pubs/articles/poliakoff\\_g/lessons\\_from\\_andrew\\_iniki.pdf](http://www.becker-poliakoff.com/pubs/articles/poliakoff_g/lessons_from_andrew_iniki.pdf) > one of the key lessons from Andrew was that the insurance industry needed to be better prepared to cope with widespread damage. In the aftermath of the 1992 hurricane, policy holders discovered in too many cases that they did not understand the limitations of the policies they had been paying for – sometimes for years. Many found that insurance payments covered only a fraction of their recovery costs. As a result, government agencies worked with insurance providers to improve coverage and clarity – sometimes with regulations imposed by appropriate agencies.

Another failing that was uncovered – sometimes literally – by Hurricane Andrew was that slipshod construction causes terrible damage in storms like Andrew. Apparently some government regulators had fallen into cozy arrangements with local builders and failed to enforce even the limited standards that might have helped reduce damages and costs. The decisions by many insurance companies to declare bankruptcy or to terminate coverage for undamaged homes infuriated residents.

So what are some of the lessons that have become standard thinking in the wake of Andrew? The Master's of Public Administration program < <http://mpa.norwich.edu> > at Norwich University < <http://www.norwich.edu> > in Vermont includes two courses that bring students into detailed discussions of today's standards.

The BC511 course, "Continuity of Government Operations," is the first of two dealing with these essential matters; major topics include the following:

- Organizational analysis
- Risk and threat analysis
- Mitigation and control strategy development
- Implementing organizational structure

A necessary component of all business continuity programs is to understand clearly who does what and why in each organization. A culture of inclusion and free exchange is essential for successful planning and implementation.

Risk and threat analysis allows us to allocate resources rationally. Evaluate which components of the critical infrastructure your organization must coordinate with. Get to know the people in your areas of responsibility. Learn their priorities.

Look at a variety of threats and evaluate how each could affect the critical components of the systems for which you are responsible. Although you may not be able to derive precise probabilities for different types of damage, you can still get a sense of likelihood from published or historical records. Don't worry about imprecision – these probabilities are just part of a method for setting priorities.

The annualized loss expectancy, or ALE<  
[http://www.riskythinking.com/glossary/annualized\\_loss\\_expectancy.php](http://www.riskythinking.com/glossary/annualized_loss_expectancy.php) >, is a useful tool for estimating (that is, doing better than just guessing wildly) at the level of investment appropriate to protect different components of the systems you are including in the business continuity and disaster recovery planning. In information security, however, we have to be aware that the enormous variety of equipment, software and configurations precludes the kind of precision that actuaries have achieved in classifying risks for, say, building types. Nonetheless, ALEs do provide an excellent basis for exploring options for rational allocation of resources. Sometimes we can learn enough about risks to engage in Monte Carlo Simulation<  
[http://www.palisade.com/risk/monte\\_carlo\\_simulation.asp](http://www.palisade.com/risk/monte_carlo_simulation.asp) > to arrive at overall probability distributions that we can constructively use in ALEs.

Whenever you are planning on changes to the usual way of doing business, remember that all organizations – including public agencies – are collections of *people* who have their own ideas, expectations and comfort zones. Don't just order people to change – discuss the issues and gain their support. Listen honestly and openly to what they have to say – after all, they are experts in their own work and actually know much more about the details than a manager from several levels above or from a different agency.

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

- Developing response plan
- Emergency operations centers
- Emergency communications
- Working with first responders
- Best practices for
- Developing off-site backups
  - Offsite work areas
  - People and equipment for continuing operations

*I'll look in more detail at these topics in the third of these columns.*

*For additional readings, see*

- DHS (2011). “Critical Infrastructure.” <  
[http://www.dhs.gov/files/programs/gc\\_1189168948944.shtm](http://www.dhs.gov/files/programs/gc_1189168948944.shtm) >
- Kabay, M. E. (2009). “Understanding Computer Crime Studies and Statistics, v6.”<  
[http://www.mekabay.com/methodology/crime\\_stats\\_methods.pdf](http://www.mekabay.com/methodology/crime_stats_methods.pdf) >
- Poliakoff, G. A. (2004). “Lessons of Andrew and Opal: Implementing a Disaster Plan.”<  
<http://www.becker->

[poliakoff.com/pubs/articles/poliakoff\\_g/poliakoff\\_lessons\\_of\\_andrew.pdf](http://poliakoff.com/pubs/articles/poliakoff_g/poliakoff_lessons_of_andrew.pdf) >

- US National Weather Service (1993). "Hurricane Andrew: South Florida and Louisiana: August 23-26, 1992." Available as e-book and on paper. <  
<http://www.worldcat.org/title/hurricane-andrew-south-florida-and-louisiana-august-23-26-1992/oclc/29973581> >

\* \* \*

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/>>

Copyright © 2011 M. E. Kabay. All rights reserved.

Permission is hereby granted to *InfoSec Reviews* to post this article on the *InfoSec Perception* Web site in accordance with the terms of the Agreement in force between *InfoSec Reviews* and M. E. Kabay.