BP, Information Security and DRP

The ongoing oil catastrophe has lessons for banks' disaster recovery plans and testing, especially if you've never had a test fail

* * *

There I was, watching an update on the BP oil rig situation when an executive from BP (he who shall not be named) conveyed to the audience that the problem was at 5,000 feet and had not been done before! It was a moment that, had I been there, would have most certainly evoked follow-up questions from me in regard to a disaster recovery plan. The questions that came to mind were: Do you have a disaster recovery plan for an event 5,000 feet? Does your plan implementation establish a central command and control structure with the authority to act? Have you practiced this plan? Do you have resources positioned to respond to such an event? Oh, by the way, I think I read on CNN that BP is going to decide on the top-kill procedure once the testing has been completed. Shouldn’t you have already done that?

Please, let me run the congressional hearings!

This oil spill is a huge tragedy for the families of those lost and for the Gulf Coast. All of it could have been prevented with vigilance and preparation, but that did not occur.

There is a lot to be learned from this event. Everything that the rig operators and BP were relying on to protect from such an event failed—from the rig’s drilling operations where the down-hole interlocks failed to prevent the gas from rising up the drilling pipe, to the cut-off valves on the floor of the sea bed designed to turn off the flow of oil. With the failure of those two systems, came the event response—or the lack thereof. It has been three weeks and oil is still flowing! This is not a funny situation. It is a cascading calamity that is growing by the day.

For perspective sake, do you have a comparable disaster brewing in your banking organization? Have you taken information security and disaster recovery seriously? Do you have a viable plan and have you tested and practiced your plan? If not, are you relying on information security measures to protect your information and systems that will fail when stressed? When was the last time you had a disaster recovery test fail? Have all of the reports from the team been reports touting success, compliance, and all of the other words that BP used when they reported on their plans? Is your fall-back plan predicated on just unplugging the equipment if you can’t turn the data leak off?

Food for thought: There are an estimated 5,000 barrels a day spilling into the Gulf, but information can leave your organization unseen and at the speed of light if compromised! It doesn’t take long to lose everything at that rate. Perhaps you should take a hard look at your Information Security and DRP plans and try to break them. It would be a good idea to find out what happens when everything fails.

— Dan Fisher, The Wombat!

About the Author

Dan Fisher is president and CEO of The Copper River Group, a consulting firm headquartered in Fargo, N. D., that focuses on technology and payment systems research and consulting for community financial institutions. For nearly 30 years, Fisher has worked in the financial industry using technology to improve the bottom line. He was CIO of Community First Bankshares (now part of BancWest), has served as a director of the Federal Reserve Board of Minneapolis, the chairman of the American Bankers Association Payment Systems Committee, and was a member of the Independent Community Bankers of America Payments Committee. Fisher has written numerous articles on banking technology and the payments system. He has authored or co-authored six books and recently published a book titled, "Capturing Your Customer! The New Technology of Remote Deposit." You can contact Fisher at dan@copperwombat.com.

P.S. To understand Dan's nickname, check out "About the Wombat" on his website, www.copperwombat.com