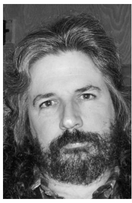
ROBERT G. FERRELL

/dev/random: a debatably helpful guide to IT disaster planning



Robert G. Ferrell is an information security geek biding his time until that genius grant finally comes through.

rgferrell@gmail.com

HOT TOPICS COME AND GO ON A VERTIGO-INDUCING rotation in IT. Sometimes one will gain popularity because of some blog post or news story; other times they seem to be generated out of thin air, apropos of not much. Nothing brings the theme of disasters into the forefront quite as effectively as a bona fide "there but for the grace of the Flying Spaghetti Monster go I" event like a plane crash or oil spill. Or maybe a plane crashing *into* an oil spill. During an earthquake. After being shot down by a rogue Predator drone whose unencrypted data stream was hacked by the widow of a Nigerian Deputy Finance Minister trying to leave you her husband's ill-gotten millions while dying of cancer. Dressed like Lady Gaga.

In IT, though, we seldom call a spade a spade, preferring content-free technical jargon like "wireless earth displacement unit," so we sequester the rather inelegant concept of disasters in a rich, velvety coating of Business Continuity Planning. That's a lot less likely to spook the stakeholders. Let us now suppose, for the sake of stretching this column out to an acceptable length, that after 24 straight hours of Anderson Cooper total immersion your CEO finally decided to jump on the Business Continuity bandwagon and you got elected to lead the orchestra. The path to BCP enlightenment is about as smooth as a drug-runner's illicit jungle runway after a meteorite shower, but fortunately I'm here to provide you with an insider's knowledge of at least the lefthand side of the equation. I've been involved in more disasters than the Great Dirigibles' Last Flights Reenactment Working Group.

BCP is a lot easier if you skip the boring stuff about RPOs, RTOs, crisis management command structures, and so on, and plunge headlong into the disaster itself. Planning a proper disaster is lots more work than most people realize. They get so wrapped up in the before and after details that they put almost no effort into implementing what is, after all, the raison d'être for the entire process. All you really need to get a good disaster going is something worth losing and plausible deniability for your involvement in said loss. Ferrell's First Law of Business Entropy states that, once set into motion, all systems tend toward catastrophic failure.

The first and foremost priority for IT disaster planning is risk analysis. If you have functional IT equipment a fair amount of risk is present right out of the box, so *that* one is something of a no-brainer in my book. The successful disaster will be well mapped out beforehand. Which servers will be involved? How many hard drives? What percentage of your organization's irreplaceable data will be lost? Whose jobs will be on the chopping block so management appears to be taking this seriously? Which senior executive bonuses, if any, will be affected, and by how much? How will you make it up to them under the table? It is critically important that the culpable party or parties be identified well in advance so that public statements can be crafted and ready for release once a suitable "incident investigation" interval has passed.

Essential logistical planning completed, the project can now move on to the implementation phase. This is where operating system patches are ignored or not properly tested on a non-production system before deployment, hardware is placed in thermally suboptimal environments containing lots of aerosolized particulate matter, and data centers are strategically located on active fault zones, in flood plains, on the slopes of questionably dormant volcanoes or, if you want to go for the trifecta, all of the above. Improperly configured firewalls and lack of an IT acceptable-use policy, anti-malware guards, or safe surfing briefings will be of great assistance during this phase.

The disaster sequence itself doesn't require much participation from the staff. As with death, taxes, and bad legislation, it just happens. It is possible and in fact advisable to influence the timing, however. Those who will be involved in the recovery effort are probably going to want to arrange it such that they can claim maximum overtime/comp time as a result. Senior management will need to minimize negative publicity, so popping on the heels of some much more newsworthy calamity is ideal. The hourly consultants who will invariably be called in to lend the impression that people who actually know what they're doing are on the case will, of course, want to drag things out as long as possible. Juggling these somewhat competing priorities is a challenge that may itself require outsourcing. It should be noted that infinite recursion is a distinct hazard where consultants are concerned.

The aftermath of an IT meltdown can be a fruited plain, ripe for the harvest, if handled correctly. A surprising number of suddenly untraceable assets may be written off, as well as any accounts payable that the payees don't realize they now need to pursue much more aggressively. With a little luck and some skilled wringing of hands you can slough off a sizeable chunk of that pesky indebtedness. Disasters can also put the *amor* in *amortize*. Subpoenas to testify before Congress are worth more than their weight in gold. By the time you finish exploiting the resulting talk show circuit and bestseller list for a few months you'll more than likely have forgotten exactly what the hoo-ha was all about to begin with. Fortunately, they say that vast amounts of money are a great balm for the amnesiac.

Caveat: inattention to detail can ruin a good disaster. For example, installing adequate uninterruptible power supplies, religious patching, and other solid configuration management practices can be extremely deleterious for failure. Another potential kiss of death for IT Armageddon is the practice of periodic off-site backups, although this threat can be ameliorated somewhat if the archive media aren't being checked for integrity or the courier regularly leaves your backups in plain sight on his car seat while he runs into the local pub for a quick one or four.

If you follow my guidelines carefully, you can be almost totally assured of an organization-altering IT cataclysm and national press attention. After all, if you're going to have a disaster, why skimp? Anything worth doing is worth doing spectacularly badly.

Bon calamité.