Herding Cats:
The Breach You Didn't Expect

March 2009

BrandenWilliams
SECURE BUSINESS GROWTH

Can you believe it has been a year? If you have read Herding Cats from the beginning, this is now the thirteenth time I have subjected you to my nonsense. Thank you for reading!

With that out of the way, let's explore the security implications of Business Continuity Planning and Disaster Recovery (BCP/DR).

We just got our first severe weather scare of the year in Texas. A tornado was reported less than five miles from my house by spotters on February 11th. Some of my customers have facilities in Tornado Alley and have heavily fortified their data centers to take a direct hit by a tornado. Usually, the secondary data center is also in Tornado Alley.

Why would you put two data centers in harms way? When you run the probability calculations, the likelihood of both being destroyed is about the same as an intersection in Montana having a Starbucks on every corner[1].

Other parts of the world have different types of concerns like earthquakes, cyclones, and monsoons. Any of these events could easily damage or wipe out a company's operations. Companies that still believe it won't happen to them will be dealt a swift lesson in humility should an event catch them unprepared[2].

The events of September 11th reminded us of an aspect of BCP/DR that we often overlook. What do we do with all the items that are not destroyed in a catastrophic event? Nature does strange things. Who would have imagined that a data theft could occur from papers flying around Manhattan after the towers came down?

Here are some of the things you need to think about when working on your BCP/DR plan.

Set up your recovery site appropriately. If your business is such that you can survive well without a particular site for a few days, then a hot site setup is not required. If you do need a hot site, then you must consider the physical and electronic security implications of synchronizing data.

Secure the backup site. If you choose to use a hot site for immediate failover, you must treat the hot site the same as your primary site. You should ensure the same level of physical security exists there to prevent burglary or theft, and that you have secured the data in transit between the sites to prevent electronic theft. Hot sites without live processing present so many challenges that several of our customers prefer to load balance between sites instead of having a primary and failover.

Reduce or eliminate risk to physical assets. If your location is in a disaster zone and sustained damage, looters will not be far behind. This means that whatever walls you depended on to keep your location secure may be damaged or destroyed. If someone is wading through a parking lot and happens to notice some nice computer equipment ready for the taking, they may be motivated to take it. Depending on where it ends up, that could easily spell a breach! Any physical asset that is at your location could be stolen. Don't leave those mounds of paper records lying around for the taking.

Make sure your communications hub is on alert. HAM Radio operators will tell you that

FOOTNOTES

[1] OK, I'm going out on a limb here… if I'm wrong, just disregard the analogy and pretend like this would never happen.

[2] See my recent blog post on Rolling the Dice with PCI for another look at the same problem.

when all else fails, amateur radio will get through[3]. Depending on your requirements, it might be a good idea to have a scanner tuned to local emergency response and amateur radio frequencies[4] for a localized disaster. You may even decide to invest in GMRS[5] equipment to keep your emergency personnel in touch in a localized area if your cell phone fails.

Have supplies! Katrina devastated New Orleans. But during the crisis, one internet provider stayed alive, and the guy in charge blogged about it[6]. Read about his adventure and you will get an idea about what kinds of supplies you might need.

Remember that in times of economic crisis, small incidents are magnified. Is your company well positioned to survive a disaster caused by nature? If not, now is a good time to revisit and make sure your board has all the information they need in order to make the best decision for the business.

FOOTNOTES

[3] *I am also guilty of saying this and chasing an occasional storm or two.*
[4] *Including Skywarn: http://www.skywarn.org/*
[5] *http://www.gmrs.org/*
[6] *http://interdictor.livejournal.com/*

About the Author:

Branden R. Williams, CISSP, CISM, CPISA/M, has been making a name for himself in the Information Technology and Security arena since 1994, as a high school Junior. Now, a graduate of University of Texas, Arlington earning his BBA in 2000 with a concentration in Marketing and the University of Dallas, where he earned an MBA in Supply Chain Management & Market Logistics, in 2004, Williams is sought after as both an Adjunct Professor and Information Technology & Security Strategy Leader in the corporate world.

Williams regularly assists top global retailers, financial institutions, and multinationals with their information security initiatives. Read his blog at or reach him directly at http://www.brandenwilliams.com/.

TEL 214 727 8227
FAX 214 432 6174
BLOG brandenwilliams.com
EMAIL brw@brandenwilliams.com

brandenwilliams
SECURE BUSINESS GROWTH