RobbLAW

IT Security &
Compliance Consulting

Disaster Recovery

What are your thoughts on disaster recovery planning?

By: Robert Adams, Esq.
Date: October 17, 2016

Disaster Recovery ("DR") planning, while important, is only a subset of an overall Business Continuity ("BC") strategy so it is important to ensure both DR and BC are well prepared and complement each other. DR planning revolves around restoring data and systems in the event of a data center or other infrastructure failure. BC is a broader strategy that includes DR planning because it revolves around how the business will continue to operate with minimal or no interruptions should an outage occur. Every organization must have a full DR and BC plan and complete a review at least annually.

Many small to medium-size organizations start their DR planning by searching the Internet for a template which they take and format to match their company's branding so they can tick the compliance checkbox that asks if they have a DR plan on file. Since they downloaded *something* from the Internet, they can technically answer "Yes." As soon as they tick that box though, everyone stops thinking about the plan. No one likes to think about or plan for when the worst-case scenario happens. What those organizations are not taking into account is that by avoiding this task, they put the entire organization at risk should something happen; it could be an earthquake, a security breach, or a complete loss of the organization's data. Whatever form it comes in, disaster will happen.

Organizations make the mistake of assuming that it is good enough to have a DR plan on file because that is all that is required for compliance. That assumption is wrong! Compliance and security are not synonymous. Compliance with regulations does not equal security. An organization is not secure simply because it is compliant. A compliant organization can be insecure and a secure organization can also be non-compliant. Both are equally important but one does not provide the other. Being able to tick the "DR Plan" checkbox for compliance may mean the organization has met its legal and regulatory obligations but that does not mean the DR plan will adequately protect the organization when the unfortunate event occurs – and it will occur. It always does.

There is nothing wrong with starting based off of a template. In fact, it is a great place to start. Once you have that template though; it is time to conduct some internal research. I start by identifying every business unit within the organization even if they are not directly involved in carrying out a DR task. Select a representative from each of those business units and have a one-on-one conversation with that representative to understand how their unit operates, what their needs are, what their workflow is like, and what their priorities are during a disaster scenario. Understanding how the business operates separately and collectively is invaluable when developing a DR plan. It may even be necessary and worth the effort to bring all the representatives together to help work through any challenges or gaps identified during each individual meeting.

For example, at one hospital I worked with, their DR plan was just a template someone downloaded from the Internet. I started by meeting with representatives from the clinical staff, medical staff, administrative staff, as well as IT staff. From those meeting, I learned that the clinical staff (e.g. nurses, technicians, etc.) do not care about restoring access to the electronic medical record system, email, or anything technology based. Prior to that meeting, I would have thought the primary system for that hospital to get back online after the basic necessities (e.g. electricity, water, etc.) would have been the electronic medical record system; however, the clinical and medical staff said it was not a priority because they can treat patients on paper without access to an electronic medical record system during a disaster. That revelation changed the entire order of events in restoring IT services for the hospital. Given information like that from these meetings, I was able to reprioritize and adjust the template DR plan to allow other systems to come online before working to restore access to a system that was not as necessary as originally believed. The reworked plan prioritized restoring their network communications so their voice-over-IP phones could come back online followed by Active Directory and Exchange ahead of the electronic medical record system to help facilitate the spread of communications during a DR scenario.

Of course, just having a DR plan is not enough. It must be reviewed and tested at implementation and at least annually thereafter. The best way to review and test a DR plan is through a table-top simulation exercise. In scheduling DR table-top exercises, I recommend coordinating with the California Department of Public Health's ("CDPH") testing of California's healthcare infrastructure; what they call the Great California Shake Out. Even non-healthcare organizations can benefit from this integration because it serves as a great annual reminder to prepare for any

event that may launch an organization's DR plan. Once that event happens for real, it is too late to start googling "what to do." Start by planning now. Robb**LAW** can help.