This website requires certain cookies to work and uses other cookies to help you have the best experience. By visiting this website, certain cookies have already been set, which you may delete and block. By closing this message or continuing to use our site, you agree to the use of cookies. Visit our updated privacy and cookie policy to learn more.

SECURITY
SOLUTIONS FOR ENABLING AND ASSURING BUSINESS

What is New (and What Isn't) in Business Continuity Planning

June 6, 2019

Kevin Alvero and Wade Cassels

When Warren Buffett, CEO of Berkshire Hathaway and investor extraordinaire, released his annual letter in February he warned about the prospect of "The Big One" — a major hurricane, earthquake, or cyberattack that he claimed would "dwarf hurricanes Katrina and Michael" and inflict severe losses.[i]

Of course, while Buffett called such a mega-catastrophe "inevitable", he also conceded that it could occur "tomorrow or in decades." Such is the uncertainty inherent in disaster preparedness. Still, Buffett was not going out on a limb in his prediction. The Disaster Recovery Institute's 2019 Predictions Report included the following disasters and major disruptions:

- US financial meltdown (triggered by over-valued tech stocks combined with China downturn) leads to a global financial crisis and world-wide recession.
- A large-scale, state-sponsored cyberattack is carried out on the CNI of a G8 country.
- Terrorism returns to US with a large, coordinated attack on a US city.
- Major flooding on US East Coast leads to severe Boston-Washington Corridor business disruption over many days.
- A leading car manufacturer stops development entirely of gasoline and diesel vehicles.
- Crises in Brazil, Argentina and Venezuela persist, spreading political, economic and migration problems across the entire region.
- China expands its domination of the South China Sea with protests from neighbors but no UN action to prevent it.

Whether fire, flood, drought, earthquake, hurricane, political unrest or cyberattack, there is no place that organizations can go to be completely safe from disaster.

Amid predictions of catastrophic business disruptions from mega-disasters, it is only natural that organizations may be questioning whether or not they are adequately prepared to continue to do business if The Big One should hit. It might be tempting for some organizations to feel like they need to run back to the drawing board and redo their business continuity (BC) plans. There should be no need to do this, though, because if companies have a fundamentally sound BC plan in place, such a plan already assumes that The Big One could hit any day. With that in mind, in the first of this two-part article we review the key elements of a fundamentally sound BC plan.

However, that doesn't mean there is nothing new in the practice of business continuity planning. Indeed, the role of the business continuity practitioner is continuing to evolve, as is the way organizations define disasters and assess their potential risk. Therefore, in Part 2 of this article we will look at some emerging best practices that can help organizations maximize the value of their BC planning efforts.

Practice the Fundamentals

The best thing an organization can do to be prepared for a mega-disaster, or any kind of disaster, is to have a fundamentally sound business continuity plan in place. To have such a plan, there are four main things that must be done right.

The first is getting the support of top management. Senior management support helps to ensure that business continuity planning efforts receive sufficient resources and that those responsible for the plan have the authority to do what is needed to make it successful. Perhaps most importantly, senior management can send the message, explicitly and implicitly, that BC planning matters.

The second key ingredient is accurately determining the needs of the business as it relates to BC planning. This includes thoroughly documenting the business's processes and assets and conducting risk assessment, information which forms the basis of the Business Impact Analysis. It is also critical to establish realistic recovery time objectives (RTOs) and recovery point objectives (RPOs) so that the plan is properly designed to meet those goals.

Once needs have been defined, the next step is the actual development of the business continuity plan. At a minimum, a robust plan includes step-by-step procedures for restoring business operations and ensuring employee safety, a communications plan, and up-to-date contact information for employees and other important parties during an emergency, such as third-party vendors, government agencies, and regulators. The plan also assigns clear ownership over each piece of the plan.

Finally, a sound business continuity plan must be updated and practiced on a regular basis. This helps to ensure that the plan is based on current, accurate information, and that the people who must act in an urgent situation can do so without second-guessing, panicking, or re-learning on the fly.

An organization with a fundamentally sound business continuity plan should feel secure that it is doing a good job of protecting itself in the event of a disaster or major disruption, but there are some trends and techniques in the field that organizations should look at to see if they could be doing even better. In Part 2 of this article, we will discuss a few of these newer ideas.

This article originally ran in *Today's Cybersecurity Leader*, a monthly cybersecurity-focused eNewsletter for security end users, brought to you by *Security* Magazine. Subscribe here.

Kevin Alvero, CISA, CFE, is senior vice president, Internal Audit, Compliance, and Governance at Nielsen.

Wade Cassels, CIA, CISA, CFE, CRMA, is a senior IT auditor at Nielsen.

Copyright ©2019. All Rights Reserved BNP Media.

Design, CMS, Hosting & Web Development :: ePublishing