

Don't Worry

By Jason Ezratty and Christopher Minnick



©athy Hull

Instead, apply risk management techniques to your CW program

Picture, if you will, *Mad* magazine's Alfred E. Neuman. His vacant, dopey grin and famous "What, me worry?" catchphrase reminds us of everything that can go wrong if we take such a cavalier attitude ourselves. So the smart move is to take precautions.

In our industry, the fallout from the unexpected bankruptcy of Ensemble Chimes Global (ECG) serves as the most recent example that in business, as in life, things can go terribly wrong. As the legal details settle and companies recover from the turmoil, we are beginning to realize several lessons to be learned, or re-learned as the case may be. These lessons teach us more than just about how to predict a provider's bankruptcy, but to examine program processes for other potential disruptions and breakdowns. If you were blindsided by ECG, what other surprises await you just around the corner?

Despite the redundancies, contingencies and countermeasures you employ to avoid program disruptions, there always seems to be a gremlin anxious to show you a new problem that has not been accounted for. The various ways in which your best-laid plans might fail — those "What-if Monsters" — are what keep us up at night.

DISASTER RECOVERY

What might be described as "paranoia" in an individual is dubbed risk management in the corporation. Risk managers measure risk as the product of how bad something would be if it happened multiplied by the likelihood of its occurrence. It isn't new news — stuff happens.

In contingent workforce management programs, the large volume of people, checkpoints and monetary transactions involved equate to what risk managers refer to as "high exposure." When exposure is high, even low probability scenarios are inevitably bound to turn up. Put in more positive terms, considering all the lottery tickets purchased, somebody is likely to win, even though the chances for any one individual are so remote.

In the Six Sigma process improvement methodology, the what-if worrying exercise is more formally referred to as a failure modes and effects analysis (FMEA). In an FMEA, what-if scenarios are listed as comprehensively as possible and then scored with respect to severity (how bad it would be), frequency (how often it's likely to happen) and detectability (how likely we are to know when it's happening).

Potential problems that contain all three qualities — severe, frequent and detectable — are typically well-accounted

for in mature contingent workforce management processes. Notorious examples that are now commonly monitored include technology malfunctions, contingent worker no-shows, billing errors and unchecked bill rate hikes. Accordingly, it has become the convention to tally these failures electronically and report their summary status on periodic scorecards. Through proactive detection and decisive management, the well-equipped program owner is able to limit the frequency and severity of predictable problems.

However, as with the ECG bankruptcy and collapse, the most severe failures that will affect your program are likely to be infrequent, perhaps even without precedent, and nearly impossible to detect. This doesn't mean we should take a cavalier attitude, but it does imply that our means of addressing unforeseen blow-ups are more along the lines of Plan B type alternatives. Preparing to maintain critical operations in the face of the unpredictable, even the unthinkable, requires a view of disaster recovery that goes beyond simple data back-up routines.

It's the category of issues that a solid business continuity plan should be capable of addressing. While every possible scenario cannot be imagined and planned for, we can at least analyze what would happen if various process components were impaired or disabled. For example, it may be impractical to consider the multitude of events that might cause a systems outage (e.g. blackout, striking ISP employees, terrorist activity, etc.), what's important is to consider what alternatives you have in the event that it occurs (e.g. fail-over set-ups, back-up manual process support).

PREPARING FOR THE WORST

It's as easy to dismiss low-probability, high-severity risks as it is dangerous. Think about it — each of the last 10 years has seen unpredictable events that caused disruptions to contingent workforce programs: Y2K-related resource shortages, stock market crashes, the terrorist attacks of 9/11, the massive power outage in the northeastern United States, Hurricane Katrina, the 2004 tsunami in the Indian Ocean that devastated Indonesia and other Asian countries. However unforeseeable any one of these horrific events may have been, the likelihood of a catastrophic event occurring in any given year seems to be rather predictable.

Let's be clear: The disruption to a contingent workforce management program in no way compares to the devastation of the aforementioned crises; but, when devastating events

happen, they cause disruptions to critical business processes as well as people's lives. As responsible business leaders, our job is to be as prepared as possible.

Consider the following devastating hypothetical scenarios. However extreme, they serve as reminders of the infinite number of ways things can, and frequently do, go wrong and, when they do, how they have significant impacts on the processes we manage.

1. Your cell phone rings at 4:09 a.m., and your spouse implores you to stop the ringing or suffer the consequences. Your company's crisis management team brings you into a conference call with your VMS provider, who informs you that their servers are unresponsive. Symptoms point to a denial-of-service attack. As it turned out, a disgruntled, recently terminated IT employee who was replaced by a contingent worker turned his rage at your VMS supplier's data center. What's your next move? How long will it take you to recover? Who's liable?

2. You walk by your managed service program (MSP) director's unoccupied desk at 10:23 a.m. She usually arrives by 7:30 a.m. and hasn't missed a day in three years. You soon learn from a tearful colleague that your program director was in a fatal car accident on the way to the office. With no immediate replacement available and much of the program's intricacies undocumented, what is your next move? How long will it take you to recover?

3. Your Blackberry is continuously buzzing, it's 7:12 p.m., dinner is almost ready and the kids are at the table on time and with clean hands for the first time ever. You glance at the device to see what the commotion is all about. It turns out your largest Japanese staffing firm has been put on suspension by the government and none of its 600 workers are reporting for duty today. What is your next move? How long will it take you to recover? How severe are the consequences of those operations being under-resourced? What will the remedy cost?

However remote the probability of any one such scenario occurring, there are enough such scenarios possible that the need for you to respond to a similar situation is unfortunately likely. And, with the growing importance of contingent workers as a labor channel throughout the enterprise, recruiting, onboarding and billing disturbances can be crippling. Moreover, and it bears repeating at every opportunity, major disruptions to a contingent labor channel cause major disruptions to the people involved.

While this level of risk analysis may be new to contingent workforce management — likely due to the relative newness of the field — it is nothing new for people in myriad other disciplines who deal in risk every day, such as insurance, finance,

Sample Contingent Workforce Failure Modes & Effects Analysis

		S E V E R I T Y			
		Low	High		
D E T E C T A B I L I T Y	HIGH	candidate submitted above rate threshold	technology errors or lag	HIGH	F R E Q U E N C Y
	LOW	poor quality resume submissions	missed program enhancement deadlines		
	HIGH	vendor's insurance expires	wide-area power outage	LOW	
	LOW	manager-vendor collusion	bankrupt VMS/MSP provider		

law, structural engineering, and food and drug safety personnel. These fields have come to terms with the reality that "stuff happens" and the need to be prepared.

More specifically, consider the precursors that led up to the ECG meltdown. Risks were being measured and gambled on at each step. Axiom, the parent company of ECG, calculated risk when paying \$80 million to acquire Chimes, the largest MSP/VMS provider at the time. GoldenTree, the asset management company that lent Axiom more than \$130 million, calculated risk during its loan approval process, and again when triggering its call on the debt. Most specifically, about 50 program owners took a risk when selecting ECG (or its ancestral entities) as their VMS/MSP provider.

Taking risk is a vital part of doing business. But, while the rewards may be readily apparent, some risks tend to be hidden.

BUSINESS CONTINUITY PLANNING

As with anything, prevention is the best medicine. While much can be done proactively to rid processes of potential failure points, it is prudent to assume that bad things will happen. Despite every ounce of prevention, every so often a pound of cure is still required. And so, galvanized by fears of a repeat of 9/11, business continuity planning quickly became common practice.

The fundamental aim of a business continuity plan (BCP) is to establish processes to:

1. Determine what actually happened to cause the problem.
2. Assess impact of the event on business (both critical and non-critical functions).
3. Enact relevant contingencies and countermeasures to ensure safety of personnel and maintain business processes in order of criticality.

4. Communicate business continuity activities to employees, customers, suppliers, shareholders and the media, as appropriate.

5. Monitor and report progress and resource utilization.

A BCP is a serious undertaking and is typically beyond the scope of any one CW program owner. However, too often the enterprise-wide BCP doesn't give proper weight or detail to CW program operations. In this case, it is up to you to identify and mitigate risks that threaten business continuity. From systems and physical infrastructure components to the various legal implications of your countermeasures per regional jurisdiction, there are many people who need to weigh in on a BCP — even if only for the CW program.

Fortunately, if you have assembled stakeholders (e.g. IT, legal, HR, security, finance, procurement) for your program, you are already talking to the right people. In the best-case scenario, BCP activities, including plan renewal, would be spelled out and agreed to within a program charter. In addition to your internal stakeholders, third-parties such as MSP/VMS partners and agencies need to be considered. In fact, your BCP should stipulate the need for these companies to have a functional BCP themselves. In addition, these third-parties may have experience dealing with some of these scenarios (or similarly catastrophic examples) and can provide valuable input.

A positive byproduct of constructing and documenting a BCP is that the exercise prompts the evaluation of your processes and their supporting infrastructures. Invariably, you will discover inefficiencies in your business, such as low-value tasks, waste and re-work simply as a result of inspection. To gain this type of perspective, it is typically best to summarize processes in graphical form using applications like Visio, though low-tech and even hand-drawn versions may be equally effective. By getting your process all into a single view the problems become apparent.

Very often, the problem spots in your processes are not there by design. They are the little Band-Aids, the exceptions to the rule that somehow became the rule, and shifts made to accommodate new technology that now, in aggregate, no longer make sense. If your organization does not follow a regular schedule of process re-examination, a BCP exercise may provide just that.

Most important, however, is that a BCP is only as good as your ability to execute it. As such, it is vital to test your BCP — and not just once, but at least annually, because we know that process inputs and resources shift over time. If your company does not test its BCP, you should at least test the portion of the BCP within your purview. Of course, if your processes' BCP is critically dependent upon other elements of the BCP going into effect (e.g. back-up generators, analog phone lines, drivable roadways), your micro-test will be at least partially incomplete.

Stuff Happens

Recent crises nobody foresaw but that affected businesses everywhere

- 1999 Y2K-related resource shortages
- 2001 Stock market crashes
- 2001 Terrorist attacks of 9/11
- 2000s Accounting scandals of major corporations such as Enron and WorldCom
- 2002 The massive power outage in the northeastern United States
- 2004 The tsunami in the Indian Ocean
- 2005 Hurricane Katrina
- 2007 Minnesota bridge collapse
- 2008 Bankruptcy of Ensemble Chimes Global

Finally, don't just let your BCP sit on a shelf. No matter how relieved you feel when the documentation initiative is done, don't forget that the "P" in BCP is "plan." It's really a starting point, to be enacted on what will likely be one of the hardest days you've ever worked.

CONCLUSION

As the adage goes, "Man plans so God can laugh." The unforeseen fallout of the ECG bankruptcy serves as our most recent example.

When considering what can go wrong and how far you should go to prevent a given disaster, cost-benefit analyses help keep a disciplined eye on return on investment. Only after considering failure modes and their potential impact, can you determine what belongs in a BCP relative to your available resources. Going broke to prevent every low probability catastrophe is as nonsensical as not thinking about them at all.

Of course, only someone with need to worry asks himself, "What, me worry?" Like an ostrich putting its head in the sand, Alfred E. Neuman is really telling us he refuses to worry despite the many concerns of modern society. In response to the Three Mile Island Accident of 1979, *Mad* magazine broke from tradition only once to have Neuman proclaim, "Yes, me worry." If Neuman can learn, any of us can. 🌐

Jason Ezratty and Christopher Minnick consult Fortune 500 companies on contingent workforce strategy initiatives such as program design, VMS/MSP selection assistance, and performance metrics analysis (www.brightfieldstrategies.com). They can be reached at jezratty@brightfieldstrategies.com or cminnick@brightfieldstrategies.com.