

BUSINESS SURVIVAL™
A Business Continuity Newsletter for Decision-makers from
ROTHSTEIN ASSOCIATES INC.

Volume 9, Issue 3

Copyright 2007, Rothstein Associates Inc.

CONTENTS

- Managing the Victim Dimension of High Profile Litigation
- Five Nines: Chasing the Chimera? by Andrew Hiles
- News
 - Bank of America Launches New Disaster Recovery Purchasing Card
 - "Software as a Service" Has Business Continuity Implications
 - Sungard Constructs Three New UK Workplace Recovery Facilities
 - Clinical Studies Provide Hope for a Pre-Pandemic Influenza Vaccine
 - Asempra Granted IT Continuity Patent
 - Senate Debates Bipartisan Bill Updating Security Act of 2007
 - Stratus Announces Continuous Availability Summit in Orlando
- Upcoming Events
- Recommended Reading

MANAGING THE VICTIM DIMENSION OF HIGH PROFILE LITIGATION

By James E. Lukaszewski, ABC, APR, Fellow PRSA

The highest priority and greatest threat, the most crucial aspect of managing crises, is the victim dimension. Victims provide the explosive emotional drive that results in high visibility, high liability, and high anxiety. Even though victimization occurs every day, and to some degree may play a role in all litigation, dealing with victims still remains among the sloppiest, most mysterious, and least well handled of all management activities.

There are seven powerful reasons why managing victims is so difficult for management and those who advise management:

1. Victim behavior is irrational.
2. Management is reluctant to promptly assume blame or responsibility.
3. Management's obsession with results over something that is clearly emotional, and by-in-large immeasurable, forces them to appear anti-victim, emotionless, and cold.
4. Management training in ethics and managing emotional circumstances is at best minimal in business schools and in business life.
5. Expectations and performance measures of managers and management advisors is generally based on rational factors.
6. Management relies on peer and legal advice to avoid apology.
7. Managers responding with empathy and sympathy can be criticized as "soft," "sentimental," even as "sissies."

In America today, the process of becoming a manager is training in de-emotionalization. Simply put, if it can't be easily measured, if it's difficult to quantify, or if it can't be metricized, it's probably not important. On top of this, managers are trained to discount, disregard, and disrespect virtually every kind of emotional expression. Peers, shareholders, and the business community expect managers to "tough it out," and "avoid looking like sissies," at least at first. It is okay to "give in" after victims have been insulted, demeaned, and slapped around a bit. The result is that management's response to crisis often comes across for what it surely is, callous, arrogant, cold, and heartless. Managers are not compensated on their level of empathy.

Going one step further, business people are taught a kind of decision-making ritual - one in which even the most urgent decisions are made through a process of conflict, confrontation, and aggressive intellectual and verbal combat. Looked at through the lens of victimization, this approach is time consuming and distracts from the humane immediacy victim response requires. Too much delay and the perceptions of arrogance, callousness, and culpability take over, especially if management hesitates or is initially hostile and negative toward victims.

In crises, one crucial strategic responsibility of company leadership is to have in place a Victim Response Unit and Special Victim Action Team, reflecting participation by communications, the Legal Department, and Human Resources, to immediately help management avoid both the collateral damage and devastating consequences of mismanaging the victim dimension; and to keep management focused on the significant benefits to reputation, public trust, and legal liability reduction that will be achieved by prompt, empathetic, and apologetic managing of victims.

Crises and Disasters Create Many Kinds of Victims

Almost every post-mortem on crisis communication failure and management decision making deficiencies identifies the failure to promptly address victims as the emotionally negative energizing force that causes trust to break down. Bad news of any consequence is about victims and victimization, or the potential for both.

When the emotionality of victimization meets the rational decision making of management, the casualties will almost always be in management.

It is helpful to differentiate between a crisis and a disaster. Crises are caused by human beings through commission, omission, accident, negligence, or ignorance. Disasters are generally natural events beyond human control - tsunamis, earthquakes, hurricanes, tornados, and incredibly powerful storms. Disasters produce victims, but unless responders act negatively, carelessly, or callously, there is far less potential for blame, bad news, or mindless victimization and collateral damage.

Who Can't Be a Victim?

Let's do some demystification. Corporations and large organizations, like government agencies, are almost never, from a public perspective, considered victims. Yes, Tylenol was a victim of a product tampering criminal in 1982 and 1986. Yes, the airlines whose planes were hijacked and flown into the World Trade Center in 2001 were victims. The syringe tampering incidents in 1993 made Pepsi, an icon American brand, a victim. The government building bombed in Oklahoma City in 1996 was also a victim. Yes, there are circumstances - although very few in number - where one could genuinely consider a large organization and its leadership to be victims. But lawyers, corporate advisors, and senior executives don't qualify.

Generally speaking, however, it is more likely that large organizations will be immediately viewed as perpetrators, or at least as having some culpability in the creation of victims. In these situations it is equally true, but perhaps not as intuitively apparent, that some employees are victims in every

scenario. If the response of the organization is to stumble, mumble, fumble, and bumble, any opportunity to be perceived as a victim is lost.

Management advisors, especially attorneys, need to recognize the crucial and important realities of the victim dimension, and be prepared to coach management for victim response readiness and for the important humane behaviors required as crises unfold.

Who Can Be a Victim?

There are three kinds of victims: people, animals, and living systems. Living systems are things like estuaries, deserts, jungles, rain forests, river valleys, or your own back yard. The fact is you can blow something up, burn something down, or destroy it, but so long as no one is injured or killed, no animals are injured or killed, and no one's living system is harmed, the situation may be bad news, but is not a crisis. Instead, it could be a disaster or simply a bad day for someone's schedule, budget, reputation, or career.

What Does It Mean to Be a Victim?

Victimhood is a self-designated state. Whether there are wounds, bullet holes, or any other visible or invisible damage, human beings have the capacity to choose to feel victimized. They can also choose to be victimized on behalf of others, like animals or other living systems.

Victimhood is self-sustaining. Being a victim is a self-perpetuating state. That is, the individual chooses how long he or she will remain in a situation or state of mind that makes him or her feel victimized.

Victimhood is self-terminating. It ends when the victims, by themselves, determine to let go of what is affecting them and get on with the rest of their lives.

No matter how damaging an event, only a small number of individuals will actually feel victimized. This is true even in mass casualty situations. While many may be injured, or disadvantaged, or require extraordinary assistance, very few blame others for their feelings of helplessness, demoralization, frustration, or betrayal. Most injured or wounded just suck it up, deal with it, and move on with their lives.

Victims suffer alone. Being a victim is an individual state. Even though there may be mass casualty circumstances where many are injured or wounded at the same time, each person suffers alone. Even the phrase "mass casualties" is a serious, potentially devastating misnomer. Every person suffers differently, experiences pain differently, and needs to be treated individually. Too often, the victimization, the sense of frustration, the sense of helplessness and being misunderstood persists because both the perpetrators and society lump individual circumstance together, too quickly. This is very frustrating to victims.

Victim Behavior Is Predictable: Key Indicators

Victims' behaviors are driven by extraordinary powerful emotion. There is anger, betrayal, disbelief, dread, and fear. There is frustration, powerlessness, and helplessness. There is inadequacy, and the agony of walking-but-wounded loneliness. In fact, these words are the vocabulary of the victimized.

Victims become intellectually deaf. When humans are victimized, the first thing that happens is the inner voice begins screaming, telling us just exactly what happened, how stupid we were, how careless we probably had to be to get into this kind of jam. Our other voice (most of us have the two voices; some of you may have more, but most of us have just two) is telling everyone else about what

you are suffering and what is happening to you. This is what often makes dealing with victims so difficult. Victims instantly become self-absorbed and self-focused on the problems and afflictions that being a victim causes. They hear little. Their inner voice continuously rehearses their problems and circumstances. They use their outer voice to complain, whine, and warn. They notice little, and they are primarily stimulated by additional negative information about their circumstances or similar ideas.

Victims are emotionally engaged 24/7. Put yourself in their place. If you are an adult, you have been victimized by something. Once it happened to you, you were consumed by it, at least for a time.

Everything is a question. Victims fail to efficiently absorb information from the outside due to their condition of intellectual deafness, victims generally ask many, many embarrassing but simple questions like, "Who's responsible?" "Why did this happen to me?" "Why couldn't this have been prevented?" "Surely there must have been some alternatives that would have headed off this problem before it happened." "Who is going to pay all my bills while I suffer these problems?" "Why didn't you warn me if you knew this could happen?"

Victim (Plaintiff) Creating Perpetrator Behaviors

Victim-creating behaviors cause most litigation. They are identifiable and preventable. Here are seven victim-causing perpetrator behaviors (I refer to these in some places as "profiles in Jell-O"):

1. **Denial:** Refusal to accept that something bad has happened; that there may be victims or others directly affected that require prompt public acknowledgement. There is denial that the crisis is serious; denial that the media or public have any real stake or interest in whatever the problem happens to be; denial that the situation should take anyone's time in the organization except those in top management specifically tasked to deal with it; denial that the problem is of any particular consequence to the organization provided no one talks about it except those directly involved. "Let's not over-react." "Let's keep it to ourselves." "We don't need to tell the people in public affairs and public relations just yet. They'll just blab it all over." "If we don't talk, no one will know."

2. **Victim Confusion:** Irritable reaction to reporters, employees, angry neighbors, whistle-blowers, and victims' families when they call asking for help, information, explanation, or apology. "Hey! We're victims too." Symptoms include time-wasting explanations of how we've been such good corporate citizens, how we've contributed to the opera, the little league, the shelter program. "We don't deserve to be treated this badly." "Mistakes can happen, even to the best of companies." "We're only human." When these behaviors don't pass the community, media, or victim straight face test, or are criticized or laughed at, a stream of defensive threats follows:

- "If the government enforces this regulation, it will destroy our competitiveness."
- "If we have to close this plant, it's their fault." "It's the only decision we can make."
- "If this decision stands, many will suffer needlessly."
- "If we didn't do this, someone else would."
- "We didn't tell them to spare them the additional agony."

3. **Testosterosis:** Look for ways to hit back, to "slap some sense" into them, rather than to deal with problems and emotional circumstances. Refuse to give in; refuse to respect those who may have a difference of opinion or a legitimate issue. There is extraordinary negative energy inside the executive circle. That's what testosterosis really is . . . an attack of abusive adrenaline. Another definitive indicator, the use of military terminology - tactics, strategy, enemy, beachhead, attack, retreat, and truce - builds a macho internal environment. This command and control mentality sets the stage for predictable errors, omissions, and mistakes, and resist to what is truly needed.

4. **Arrogance:** Reluctance to apologize, express concern or empathy, or to take appropriate responsibility because, "If we do that, we'll be liable," or, "We'll look like sissies," or, "We'll set bad

precedents," or, "There'll be copycats," or, "We'll legitimize bad actions or people," or "We can't give them what they don't deserve." Arrogance is contempt for adversaries, sometimes even for victims, and almost always for the news media. It is the opposite of empathy.

5. **Blame Shifting / Search for the Guilty:** Dig into the organization or community to look for traitors, turncoats, troublemakers, those who push back, and the unconvinced to shift the blame to them. You know it's happening when you hear these phrases:

1. "They simply weren't damaged enough to warrant the demands they're making."
2. "The allegations are outrageous, unprovable, and self-serving."
3. "Obviously, these people have their own agenda, and we have become the victim of it."

6. **Fear of Exposure:** As the bad news coverage and employee animosity persists, the media and victims begin asking, "What did you know, and when did you know it?", "What have you done, and when did you do it?", along with other humiliating, embarrassing, and damaging questions. Angry, callous responses create even more victims, or harden the attitudes of existing victims. And the plaintiffs' attorneys line up.

7. **Management by Whining Around:** When the decision is made to finally make some accommodation and move toward settlement, the organization talks only about its own pain, expense, and inconvenience. This makes victims, employees, neighbors, and the government angrier, and the media more aggressively negative, creating even more plaintiffs and accusations. Whining is never an effective strategic tool or strategy.

What Do Victims Need?

Victims have four powerful needs. If these four needs are provided promptly - preferably by the perpetrator - victims will more easily move through their state of victimization and be less likely to call or respond to attorneys, the media, or even to call attention to themselves. The reality is that if the perpetrator fails to meet their needs or does so only partially, victims will find ways to provide them for themselves, often at the perpetrator's expense.

- **Validation**, that they are indeed victims. This recognition is best rendered by the perpetrator; if not, public groups, government, or the news media will do it.
- **Visibility**, a platform from which to describe their pain and warn others. Preferably, again, the platform should come from the perpetrator, or a credible independent organization that can help the victim explain what happened, both for the purpose of talking it out and also convincing others to avoid similar risks or take appropriate preventive action.
- **Vindication**, through action by the perpetrator to ensure that whatever happened to the victim will never be allowed to happen to others. Victims rarely sue because they are angry, their life has been changed dramatically, or because lots of plaintiff's attorneys are chasing them around. Generally, victims sue because their situation is not acknowledged and their feelings are ignored, belittled, or trivialized. If they are prevented from publicly discussing what happened to them in meaningful ways, and no one is taking prompt constructive action to prevent similarly situated individuals, animals, or living systems from suffering the same fate, they will be looking to take more aggressive action.
- **Apology**, directly and promptly tends to dramatically reduce victimization and virtually eliminate litigation. While the lawyers may strongly advise against any form of apology because, under law, an apology is an admission, there is a growing body of evidence and data to demonstrate that apologies, promptly and sincerely delivered, virtually eliminate the potential for litigation. This means that while the lawyer's advice needs to be listened to, if the

victim refuses to sue, it may be time to reassign the lawyer to negotiating an effective settlement rather than pursuing a futile effort to deny what the victim needs most.

Apology and Prompt Disclosure Are Arrogance Reduction Strategies That Also Reduce Risk

An article published in *Annals of Internal Medicine* on December 21, 1999 outlined a new litigation risk reduction strategy: Keep the patient in the information loop, aggressively, constantly, no matter what, especially when mistakes and errors occur. The organization involved was the U.S. Department of Veterans Affairs. The VA's new risk management strategy was called "Extreme Honesty."

Humanistic Risk Management

For the first time, a credible organization purposely adopted a strategy designed to reduce liability, litigation, and threats to reputation, and could validate something every victim seeks to be able to do - deal honestly, openly, fairly, and truthfully with various constituencies, especially when bad things happen. In the paper's abstract, the authors discuss what they call "humanistic risk management." This includes "early injury review, steadfast maintenance of the relationship between the hospital and the patient, proactive full disclosure to patients who have been injured because of accidents or medical negligence, and fair compensation for injuries." This is trust building and maintaining behavior.

Victim Management

The greatest barrier to disclosure and appropriate victim attitude management is management's fear of liability, fostered by well-meaning but misguided counsel. Any credible way to reduce or mitigate this fear is essential to better behavior, reputation management, and litigation reduction.

The lawyer's first assumption, now well ingrained in management, is that total honesty and candor in situations of omission, commission, error, and negligence can only lead to higher liability. The data in this article tend to refute that, saying essentially that the liability performance of the Lexington facility is better than other comparable facilities that rely on secrecy, denial, even deception.

The "Extreme Honesty" article also mentioned a study published in *The Journal of the American Medical Association* in 1992 that examined why 127 families sued their healthcare providers for perinatal injuries: "Of 127 families who sued, 43 percent were motivated by the suspicion of a cover-up or by the desire for revenge. Another study of 149 randomly selected patients in an academic internal medicine practice found that almost all the respondents "wanted their physicians to acknowledge even minor errors; many stated that they would respond to an unacknowledged moderate or severe mistake by filing a lawsuit."

One lawyer interviewed for the article put it this way: "In over 25 years of representing both physicians and patients, it became apparent that a large percentage of patient dissatisfaction was generated by physician attitude and denial, rather than the negligence itself. In fact, my experience has been that close to half of malpractice cases could have been avoided through disclosure or apology but instead were relegated to litigation. What the majority of patients really wanted was simply an honest explanation of what happened, and if appropriate, an apology. Unfortunately, when they were not only offered neither but were rejected as well, they felt doubly wronged and then sought legal counsel."

If you simply substitute the word "victim" for "patient" in U.S. Department of Veterans Affairs' four-step "Extreme Honesty" process, you have the basis for a major lesson in reputation preservation for your company or organization.

Extreme Honesty: How This Process Works at the VA

The U.S. Department of Veterans Affairs uses a four-step process to notify patients of negligence:

1. Risk management committee:
 - Identifies an instance of accident, negligence, or malpractice.
 - Investigates the facts.
 - Interviews involved physicians, the chief of relevant clinical service, and other personnel.
2. If the Committee finds malpractice or substantial error (resulted in loss of patient's function, earning capacity, or life):
 - Plans are made to notify the patient or next-of-kin.
 - Patient's surrogate or next-of-kin is called (usually by the chief of staff).
 - Family is told that there was a problem with the care in question and is asked to come to the medical center at their convenience for an explanation.
 - Telephone conversation provides just enough details to indicate the seriousness of the matter (including, if necessary, a statement that a medical mistake was made and that an attorney may accompany the patient or family, if desired).
3. Face-to-face meeting:
 - With the chief of staff, the facility attorney, the quality manager, the quality management nurse, and sometimes the facility director.
 - All details are provided as sensitively as possible, including the identities of persons involved in the incident.
 - Emphasis is placed on the regret of the institution and the personnel involved; and on any corrective action that was taken to prevent similar events.
 - Offer to answer questions and an offer of restitution, along with subsequent medical or surgical treatment.
 - Assistance with filing for service connection under 38 United States Code, section 1151.
4. Claims assistance:
 - Patient, surrogate, or next-of-kin is assisted in filing the necessary forms.
 - Victim is given the names and phone numbers of persons who can answer any additional questions.
 - Patient or next-of-kin is advised to retain counsel, if they haven't all ready.
 - Committee is forthcoming to the plaintiff's attorney so that the attorney's review of the medical record will confirm the information that was volunteered.

- The facility's attorney and the patient's attorney work together to reach an equitable settlement on the basis of "reasonable calculation of loss."

Recent Developments

Saying "I'm sorry," is becoming a mainstay in healthcare communication, triggered by the healthcare insurers, who have suddenly begun to realize that apologies promptly and sincerely delivered, by all parties to an adverse medical event can significantly reduce, if not eliminate litigation. If you go to your favorite browser and click on www.sorryworks.net you'll come across a huge site involving a tremendous number of hospitals and healthcare organizations from across the United States, all of whom are joining in the chorus to urge doctors, lawyers, and medical administrators to engage in what is called in medical shorthand, the "I'm sorry" movement.

The pressure to do this is so great that in an increasing number of cases, failure to apologize promptly at the first sign of a medical problem could void a doctor's liability coverage and coverage to pay any attorney who might defend that physician or healthcare institution.

On September 28, 2005, Senator Hillary Rodham Clinton of New York and Senator Barack Obama of Illinois jointly introduced the "National Medical Error Disclosure and Compensation Act of 2005." The introduction of this legislation reads, in part, "Solutions to patient safety, litigation, and medical liability insurance problems, while challenging, are critical. In an attempt to address these issues, a number of hospital systems and private liability insurance companies around the country have adopted a policy of robust disclosure of medical errors with thorough analysis and intervention, apologies for such errors and early compensation for patient injury."

"Overall, these policies have resulted in greater patient trust and satisfaction, more patients being compensated for injuries, fewer numbers of malpractices being filed, and significantly reduced administrative and legal defense costs for providers, insurers, and hospitals where such policies are in place."

Apparently, the ability for us to significantly limit litigation in crisis situations is at hand if we remember what victims need and the powerful closure value of apology. Managing the victim dimension creates time and conserves resources to deal with whatever the remaining aspects of your crisis happen to be. And, when it comes to litigation, only three of every 100 civil cases will ever get to trial. If you pursue a litigation strategy and you actually get to court, odds are you'll be hearing the old classic, "Who's sorry now?", being sung by the victims about you.

The victimized have enormous power in our society. The lesson is - chill out. Have a heart. Listen to your guts. When there are victims, set aside your inherently adversarial training and nature, and then, pragmatically and humanely, manage the victim dimension. It's how your mom taught you to behave, anyway. And that isn't mush.

Copyright © 2007, James E. Lukaszewski, Reprinted with permission.

James E. Lukaszewski is an expert in managing and counteracting difficult corporate communications issues. The situations he addresses often involve conflict, controversy, community action, activist opposition, or leadership failure and recovery. His name has appeared in *Corporate Legal Times* as one of "28 Experts to Call When All Hell Breaks Loose," and in *PR Week* as one of 22 "crunch-time counselors who should be on the speed dial in a crisis." He is among the first 100 professionals to be certified (CCEP) as a Corporate Compliance and Ethics Professional, by the Society for Compliance and Ethics (SCCE). www.e911.com

FIVE NINES: CHASING THE CHIMERA? by Andrew Hiles, FBCI

Five nines (99.999%) availability: why chase it? "Because it's there?" Is it actually achievable? Or for a sound business reason? What's the payback? Is it some goal we strive for, like the ultimate truth or perfect beauty, that we know we are unlikely ever to attain? Or should we really be striving for six nines (99.9999%)?

Let us examine the math of it, first. A definition of availability may help: "The percentage uptime achieved per year." Given this definition, the maximum downtime permitted per year may be calculated as reflected in Table 1 below. Please do not debate with me leap years, lost seconds or even changes to Gregorian Calendar. Equally let us not debate time travel! To quote a Cypriot saying: "I am from a village: I know nothing." The figures below are sufficiently accurate to make the points this article is trying to get across.

Table 1: Uptime and Maximum Downtime

Uptime	Uptime	Maximum Downtime per Year
Six nines	99.9999%	31.5 seconds
Five nines	99.999%	5 minutes 35 seconds
Four nines	99.99%	52 minutes 33 seconds
Three nines	99.9%	8 hours 46 minutes
Two nines	99.0%	87 hours 36 minutes
One nine	90.0%	36 days 12 hours

If you really want to throw a spanner in the works, change the definition of availability to: "The percentage of scheduled uptime per year." But let's not go there. We are talking absolutes.

Figure 1 summarizes components (i.e. dependencies) just for an ICT facility, excluding ICT equipment, systems and software.

Figure 1: Calculating Availability: Facility (Source: Uptime Institute)

Specification Item	Specification
Number of delivery paths	3 active
Redundant components	2 (N+1) or S+S
Support space to raised floor ratio	100%
Initial watts/sq. ft.	50 - 80%
Ultimate watts/ sq. ft.	150+
Raised floor height	30 - 36"
Floor loading pounds/sq. ft.	150+
Utility voltage	12-15kv
Construction \$/sq. ft. raised floor	\$1100+
Annual IT downtime due to site	0.4.hours
Site Availability	99.995%

All this implies alternate power sources: for example, mains power from separate sub-stations; dual UPS; back-up generators with automatic cut-in and capacity to cover equipment and, where necessary, end-user environments, elevators etc; adequate fuel supplies.

We also need permanent - 24x7x365 - on-site support with appropriate skills, tools etc. This falls short of the fabled five nines, but it is as high as the Uptime Institute's Tier classification goes - and only 10% of organizations achieve this.

Well, let us assume we can engineer the facility (including the personnel involved in running and supporting it) to deliver a 99.999 per cent availability.

The next question is: "How do we measure the availability within our service?" Now we need to include ICT equipment, operating systems, diagnostic, performance measurement and management software, middleware, applications and anything else used in the delivery of the service. Then we need to calculate the availability of each of these components on which the service depends.

It is easy to assume that replicating components halves the downtime: but, in introducing more components, we are also introducing greater complexity and more possible points of failure. Where components have been replicated, they also need to be kept in synch and switchable between the two parallel configurations at any point of failure, so, for example, switches are introduced. If one configuration is active and the other passive, the switches detect component failure in the primary (active) configuration and switch the load to the secondary (previously passive but now active) matched component in the second configuration, which assumes the role and identity of the primary component. The result is improved resilience - but also more complexity, more components and more than double the cost.

Where there is only a single configuration, and if each component has a 99.999% availability, the theoretical availability of the overall service is calculated by multiplying 99.999% by 99.999% and multiplying the result by the availability (99.99%) for every component in the configuration. If we arbitrarily say there are ten physical components in the configuration, if my trembling finger has hit the right keys the appropriate number of times, the theoretical availability works out at "only" 99.988%. Even if we replicate all these components to the extent that we increase the configuration availability overall to 99.999% and if we manage to get the physical infrastructure (see Figure 1) to deliver 99.999% our overall theoretical capability will still "only" be 99.997%.

So far this figure represents purely infrastructure and hardware failure: we should also include the possibility of loss of operating systems, middleware, application software, databases and data. Even including these elements, the two systems need to be geographically separated since, if they are in the same data center, a fire, bomb, geophysical, meteorological or common infrastructure incident or facility failure could impact both of them. And on top of this is the security level: outage could equally well come from security breach as equipment or software failure.

Just one other point: our availability figures typically derive from manufacturer's (or maintenance companies') statistics on Mean Time Between Failure (MTBF). MTBF is exactly that: it conceals variations in actual performance and comes up with a 'normalized' performance. That is, every user of a piece of equipment with a 99.999% MTBF does not get 99.999% MTBF: some people get better performance, some worse. Microsoft claimed that its top-end Windows 2000 servers were "designed to deliver 99.999% server uptime." This is not the same as delivering it! An Aberdeen study of Windows 2000 customers running production systems reported that, on average, customers were achieving only about 99.964% uptime - about 3.2 hours of downtime per year.

Another consideration is fix time, when the equipment does fail. In the case of a single component, a 99.999% availability implies a time from fail to fix of less than five seconds! OK, you have a redundant component. Have you ever had two flat tires on a single journey? I have! You could call it Murphy's First Law of Availability.

So is 99.999% achievable? Yes. But over how long a period? A year? Two years? Five years? Seven years? Basically, unless we calculate the numbers, we are effectively walking in to a casino and betting against the bank. Sometimes we win. But over time, sooner or later, the bank always wins, according to Murphy's Second Law of Availability.

Andrew Hiles is President of Kingswell International, a consulting company specializing in business risk management and service management. He is the author of [The Complete Guide to IT Service Level Agreements: Matching Service Quality to Business Needs](#); [Service Level Agreements: Winning a Competitive Edge for Supply and Support Services](#); [Service Level Agreement Framework on CD-ROM for IT and Technology](#) and [E-Business Service Level Agreements: Strategies For Service Providers & E-Business Professionals](#). All are published by Rothstein Associates Inc.

NEWS

Bank of America Launches New Disaster Recovery Purchasing Card

Bank of America (Charlotte, NC) is introducing 'Emergency Relief Cards,' a suite of prepaid card products that will assist corporations and government entities to prepare for disasters. The special-use cards are designed to be incorporated into contingency plans to enable business continuity and to provide relief measures during times of critical need.

The new Emergency Relief product suite is built upon the knowledge gained during prior emergency situations that underscored the vital value of card programs. In the aftermath of Hurricane Katrina, Bank of America provided 200,000 prepaid cards to the Salvation Army for much needed victim relief. During the 2004 hurricane season, Bank of America issued more than 300 emergency purchasing cards to the State of Florida to deploy crews and restore roadways. These cards were used for more than 7,000 emergency purchases totaling \$7 million, and led Bank of America to develop solutions that can be set up in advance and incorporated into business continuity and disaster recovery plans. The suite of prepaid Emergency Relief cards currently includes cards that can be tailored for different situations. For example, by employing merchant code restrictions, programs can be designed with the ability to prevent card use for inappropriate purposes. Except for these merchant code restrictions, the cards may be used anywhere that Visa is accepted. Cards can also be customized for particular client requirements, including whether to allow cash withdrawals and what dollar amount is to be pre-loaded on the cards.

A new version of the card will be available this summer allowing clients to pre-order unfunded cards that can be activated and loaded with funds based upon a pre-determined contingency plan. Under this system, which is believed to be the first of its kind in the industry, card numbers, intended recipient names and pre-authorized amounts will be kept on file with the bank to be activated if and when needed. This information will be updated monthly by the client to ensure accuracy and the ability to activate the system rapidly. Additionally, duplicate emergency instructions can be provided to the bank. If a client cannot access technology systems during a crisis to enable their plan, Bank of America can initiate it for them. <http://www.bankofamerica.com/>

Source: Continuity Central, www.continuitycentral.com

"Software as a Service" Has Business Continuity Implications

The market for software as a service (SaaS) continues to pick up steam. According to Gartner the worldwide SaaS market reached \$6.3 billion in 2006 and is forecast to grow to \$19.3 billion by year-end 2011. SaaS is hosted software based on a single set of common code and data definitions that are consumed in a one-to-many model by all contracted customers, at any time, on a pay-for-use basis, or as a subscription based on usage metrics.

"The client/server era is driving alternative approaches to IT development, delivery and management, of which SaaS is the most apparent version," said Ben Pring, research vice president for Gartner. "There is now a widespread consensus among the movers and shakers of the IT industry that SaaS is an important and meaningful issue which can no longer be regarded as the 'lunatic fringe.'"

SaaS adoption is broadening out from areas such as customer relationship management and human resources into new areas such as procurement and compliance management. However, the scale of change involved in moving to a SaaS approach is proving hard for many vendors to manage, said Gartner.

Although the SaaS market is still relatively small, service providers need to make important strategic decisions and enact changes on the technology to keep ahead of the SaaS wave:

- Use solutions built on next-generation Web services, SOAs and highly automated server farms to produce multi-tenant, mass-customizable solutions that facilitate agility while sustaining uniqueness at a reduced cost.
- Make strategic decisions around whether to offer SaaS as simply one element of a broader portfolio or to fully evolve toward a SaaS-based delivery model.
- Act now because of the scale of change required to successfully exploit SaaS opportunities.
- Conduct thorough due diligence to be well-placed to take advantage of opportunities and manage risk as the market evolves toward SaaS.

From a business continuity perspective, the move to SaaS changes the vulnerability profile for software applications. When applications are run in-house day-to-day vulnerabilities are limited to the availability of the firm's own computing infrastructure. Under a SaaS environment these vulnerabilities remain, but, in addition, application availability becomes dependent on the provider's computing and delivery infrastructure. A further issue also arises; that of the financial viability of the provider company, especially where special software is provided by a smaller supplier. If the SaaS goes out of business, the software being provided will become permanently unavailable; possibly with no prior notice whatsoever.

www.gartner.com

Source: Continuity Central, www.continuitycentral.com

Sungard Constructs Three New UK Workplace Recovery Facilities

SunGard Availability Services (Wayne, PA) has announced the construction of three new workplace recovery centers in the UK. The new sites will have a combined area of over 153,000 square feet and will provide 1,660 new workplace recovery positions. The centers are located in Elland, West Yorkshire; Leatherhead, Surrey; and Milton Keynes, Buckinghamshire. They increase the total number of SunGard workplace recovery positions in the UK beyond 10,000.

Each center will feature several recovery suites, each offering between 10 and 100 workplace recovery positions. All SunGard workplace recovery facilities offer standardized telephony, PCs, printers, LAN switching and servers as well as fully cabled meeting rooms, conference facilities, kitchen and rest areas.

Linking the three new sites is SunGard's National Network (SNN), which interconnects SunGard's regional recovery facilities, and links them to SunGard's primary data center, the London Technology Center. From here, the network extends across ScaleNet, SunGard's optical network, to SunGard's London recovery locations, thereby creating a UK-wide virtual recovery campus of over 20 facilities.

In the event of wide-scale or multiple disaster declarations, when a customer's first choice recovery location may be rendered unavailable, the SunGard network infrastructure, combined with SunGard's workplace recovery offering at each of its workplace recovery centers, helps SunGard offer customers the use of available, alternative SunGard UK workplace recovery sites - referred to as 'rollback' facilities. www.sungard.co.uk

Source: Continuity Central, www.continuitycentral.com

Clinical Studies Provide Hope for a Pre-Pandemic Influenza Vaccine

GlaxoSmithKline (Brentford, Middlesex, UK) has published clinical trial data from two new studies, which show, for the first time, that GSK's candidate pre-pandemic split antigen H5N1 vaccine, formulated with GSK's proprietary adjuvant system, provides a substantial level of cross-immunity against a 'drifted' (diverse) strain of H5N1. It is hoped that the immune response elicited with this vaccine, could help prepare, or 'prime', the immune system to rapidly respond against variants of the H5N1 strain and therefore protect the vaccinated population in the event of an H5N1 human pandemic.

Key Points From GSK's Clinical Trials Report

In the first study presented at the IX International Symposium on Respiratory Viral Infections (ISRVI), data demonstrated GSK's proprietary adjuvanted candidate pre-pandemic vaccine, containing very low levels of the Vietnam H5N1 antigen (3.8 micrograms), elicits a strong cross-immune neutralizing antibody response in humans against the Indonesian strain of the virus. GSK's proprietary adjuvant system also displays powerful antigen-sparing properties. This could mean, in effect, that by adding GSK's proprietary adjuvant system, vaccine manufacturing capacity could be increased more than tenfold. The vaccine was shown to have an acceptable safety profile when compared to the control group. As expected, reactogenicity (injection site tenderness) was slightly higher in the vaccine group due to the use of the adjuvant system.

In a second study presented at ISRVI, the data showed that GSK's proprietary adjuvanted pre-pandemic vaccine could protect against two diverse H5N1 flu strains, again at very low levels of antigen. The in vivo data from the pre-clinical studies demonstrated that GSK's adjuvanted vaccine, containing the Vietnam H5N1 strain, was not only able to protect against challenge with the vaccine virus strain, but also provides 96% cross- protection against a lethal challenge with the drifted Indonesia strain of H5N1, giving an additional boost to hopes that pre-pandemic vaccination is a viable strategy for inclusion in pandemic preparedness plans.

Jean Stephenne, President, GlaxoSmithKline Biologicals, the vaccine division of GSK, said, "I am extremely encouraged by the new trial data that has been reported on GSK's candidate pre-pandemic influenza vaccine. The data confirm that our pre-pandemic influenza vaccine has the ability to recognize and kill an H5N1 strain that is different to the one contained in the vaccine. This means that proactive administration of our pre- pandemic vaccine before or just after the start of the pandemic could help to substantially slow down the spread of disease." Relenza and Daronix are registered trade marks of the GlaxoSmithKline group of companies. www.gsk.com

Source: Continuity Central, www.continuitycentral.com

Asempra Granted IT Continuity Patent

Asempra Technologies (Sunnyvale, CA), a provider of instantaneous application and data availability solutions for Windows-based environments, recently received a U.S. patent (No. 7,096,392) for 'a method and system for automated, no downtime, real-time, continuous data protection.' Asempra's next-generation file continuous data protection technology provides guaranteed application and data availability for Windows environments. Using 'Virtual On-Demand Recovery' technology, an application's data is available for use within minutes, even seconds, of recovery. The data recovered is guaranteed to be completely usable on the first recovery. With Asempra's 'Business Continuity

Server', simple point-and-click global-to-granular recovery provides recovery flexibility that ranges from individual objects, such as a single e-mail or file, all the way to a complete data center.

Asempra claims it has reduced the cost and complexity of mid-market IT data protection by consolidating the needs of backup, IT continuity, disaster recovery, recovery management, compliance and governance into just one tool. "This patent demonstrates the strength of our approach to continuous real-time data protection and our focus on delivering unmatched instantaneous application and data availability," said Siew Sim, CTO and co-founder of Asempra. "The Asempra Business Continuity Server provides file-based continuous, application-aware protection that is a perfect solution for commercial, mid-market companies that need a data protection solution that insures maximum data reliability, selectability, and dramatic cost reductions compared to today's data protection products." www.asempr.com

Senate Debates Bipartisan Bill Updating Security Act of 2007

Calling for the U.S. Senate to act with a sense of urgency, Homeland Security and Governmental Affairs Committee (HSGAC) Chairman Joe Lieberman, Ind-CT., and Ranking Member Susan Collins, R-ME, recently called for debate on S.4, a bill to improve the nation's security against terrorism by fully implementing the 9/11 Commission's recommendations. "Every day that we don't act is another day in which we are not as secure here at home as we should be," said Lieberman. "This bill would create a strategy to strengthen our homeland security against the threat of terrorist attack and also prepare for and recover from all hazards, whether natural or man-made. We've studied. We've reflected. And now, with a real sense of urgency, it is time to act to build a safer and more secure nation for the generations to come." Said Senator Collins, "This legislation continues the work of Congress and the Senate Homeland Security Committee to strengthen our homeland security in the spirit that shaped the recommendations of the 9/11 Commission. Our legislation's broad-front attack on the threats we face will ensure good value for every dollar our nation spends to improve our defenses at the federal, state, and local levels. The legislation would ensure significant and predictable funding for our state, local, and tribal governments to help safeguard our lives and properties in all catastrophes, whether natural or manmade. And it will strike an appropriate balance between increased security and our cherished civil liberties."

The bipartisan bill, Improving America's Security Act of 2007, would provide risk-based homeland security grants to states, create a dedicated interoperable communications grants program for first responders, restrict terrorists' ability to enter the United States, and improve information sharing among federal, state, and local officials. It also includes provisions to strengthen privacy and civil liberties.

Source: House Committee on Homeland Security

Stratus Announces Continuous Availability Summit in Orlando

Stratus Technologies, Inc. (Maynard, MA) will launch what it claims is the first technology industry event to focus on continuous availability computing when it kicks off the Continuous Availability Summit 2007 on March 25 in Orlando (same dates as Disaster Recovery Journal's DRJ Spring World). The three-day event will focus on the growing corporate need to support mission critical applications with failure-proof network infrastructures that resist unscheduled downtime.

The summit features practical lessons and insights from companies that have achieved 'five nines,' or 99.999 percent network availability, and from leading analyst firms such as Forrester, IDC, and others. End-user speakers will be drawn from international firms and agencies in areas such as manufacturing, telecommunications, utilities, banking, public safety, etc. to present at more than 30 breakout sessions on March 26 and 27. They will speak on topics including: security breaches; building infrastructures with no single point of failure; information lifecycle management to meet regulatory requirements; and holistic approaches to continuous availability.

In addition to the breakout sessions and keynote speeches, the Continuous Availability Summit 2007 includes a panel discussion on virtualization moderated by an IDC analyst, and an exhibition of continuous availability solutions. The Summit intends to provide non-partisan advice for achieving 99.999 percent availability. That issue promises to grow more important as businesses rely on technology systems to generate revenue and meet customer expectations for 24x7 service.

Current sponsors include Microsoft, Alaric, Postilion, Sightline and DRA. Dell is providing delegate Internet kiosks. For more information, see <http://www.stratus.com/summit/index.htm>

UPCOMING EVENTS

March 2007

25-28: **Spring World 2007 (Disaster Recovery Journal)**; Orlando, Florida, USA

www.drj.com

26-30: **Business Continuity Awareness Week – Europe**

www.thebci.org/bcaw.htm

28: **Continuity Forum Conference**; Sydney, Australia

www.continuity.net.au

28-29: **Business Continuity - The Risk Management Expo 2007**; London, UK

www.businesscontinuityexpo.co.uk

April 2007

12: **Disaster Preparedness Summit**; Houston, Texas, USA

www.disasterpreparednesssummit.org

12: **NEDRIX Hurricane Simulation Exercise**; Quincy, Massachusetts, USA

www.nedrix.com/conference.html

17-18: **World Continuity Congress**; Singapore

www.worldcontinuitycongress.com

20: **Survive: Implementing BS 25999 – the Business Continuity Standard**; London, United Kingdom

www.survive.com/training

22-25: **Strohl Systems User Group Conference**; Phoenix, Arizona USA

www.strohlsystems.com

23-25: **Continuity Insights Management Conference**; New Orleans, Louisiana, USA

www.continuityinsights.com

24-25: **DRI Asia 2007**; Singapore

<http://www.driasia.org/>

30-May 3: **Disaster Forum 2007**; Banff, Alberta, Canada

<http://www.disasterforum.ca/>

May 2007

4: **Disaster Preparedness Summit**; New Orleans, Louisiana, USA

www.disasterpreparednesssummit.org

7-13: **Business Continuity Awareness Week - Americas and Australasia**

www.thebci.org/bcaw.htm

17: **Disaster Preparedness Summit**; Chicago, Illinois, USA

www.disasterpreparednesssummit.org

22-24: **CPM 2007 West (Contingency Planning & Management)**; Las Vegas, Nevada, USA

www.contingencyplanning.com

24: **Survive: Combining Business Continuity and Risk Strategies**; London, United Kingdom

www.survive.com/training

June 2007

6: **Survive: Implementing BS 25999 – the Business Continuity Standard**; London, United Kingdom

www.survive.com/training

12: **NEDRIX Summer Conference**; Nashua, New Hampshire, USA

www.nedrix.com

July 2007

8-11: **17th World Conference on Disaster Management**; Toronto, Ontario, Canada

www.wcdm.org

17-18: **Business Continuity 2007: Building the Resilient Enterprise**; New York, NY USA

www.cio.com/bc_2007

RECOMMENDED READING

*These and hundreds of other books, software tools, videos and research reports are available from **THE ROTHSTEIN CATALOGS ON DISASTER RECOVERY AND SERVICE LEVEL MANAGEMENT** at **www.rothstein.com**:*

ROOT CAUSE ANALYSIS HANDBOOK: A GUIDE TO EFFECTIVE INCIDENT INVESTIGATION, by Risk & Reliability Division, ABS Group, Inc.

ROOT CAUSE ANALYSIS HANDBOOK: A GUIDE TO EFFECTIVE INCIDENT INVESTIGATION presents a proven system designed for investigating, categorizing, and ultimately eliminating, root causes of incidents with safety, health, environmental, quality, reliability, and production-process impacts.

Defined as a tool to help investigators describe what happened, to determine how it happened, and to understand why it happened, the Root Cause Analysis System enables businesses to generate specific, concrete recommendations for preventing incident recurrences.

Using the factual data of the incident, the system also allows quality, safety, and risk and reliability managers an opportunity to implement more reliable and more cost-effective policies that result in major, long-term opportunities for improvement. Such process improvements increase a business' ability to recover from and prevent disasters with both financial and health-and-safety implications.

Special features include a 17 inch by 22 inch pull-out Root Cause Map, a powerful tool for identifying and coding root causes.

The book helps readers to understand why root causes are important, to identify and define inherent problems, to collect data for problem solving, to analyze data for root causes, and to generate practical recommendations.

<http://www.rothstein.com/data/dr388.htm>

INFORMATION SECURITY POLICIES MADE EASY:
A COMPREHENSIVE SET OF INFORMATION SECURITY POLICIES
Version 10 (Book + CD-ROM) by Charles Cresson Wood

Information Security Policies Made Easy is the definitive, best-selling information security policy resource by Charles Cresson Wood, CISSP, CISA, CISM. Based on the 25 year consulting experience of Mr. Wood, ISPME is the most complete security policy resource available. Version 10 contains over 1360 pre-written information security policies organized in ISO 17799 format on a fully linked and searchable web based CD-ROM. Take the work out of creating, writing, and implementing security policies.

"This is the gold standard Policy reference for any serious security practitioner to have in their arsenal of tools, a must have! The instructions and examples for establishing security polices and implementation processes add real value to this edition." - John B. Kramer, CISSP, CISA, Information Security Manager - UPMCHS

<http://www.rothstein.com/data/dr303.htm>

ROTHSTEIN ASSOCIATES INC.

4 Arapaho Rd., Brookfield, CT 06804-3104
203.740.7400 or 1.888.ROTHSTEIn; fax 203.740.7401
email: newsletter@rothstein.com

www.rothstein.com

Newsletter Editor: Paul F. Kirvan, FBCI
Executive Editor: Philip Jan Rothstein, FBCI
Copyright 2007, Rothstein Associates Inc. All Rights Reserved

BUSINESS SURVIVAL™ is sent *ONLY* by YOUR subscription request!
To unsubscribe: email newsletter@rothstein.com, subject "UNSUBSCRIBE-BSN."