Four Lessons that should Change Your Business

One Goal that should Drive It: Survival!

By Dave Patterson and Dietmar Kubasta

In providing high-end IT solutions to over five hundred medium and large-size corporations, we sometimes disagree with a customer over IT security strategies. This includes improved security policies, virus protection, and intrusion detection, firewalls, high availability solutions, and more secure hardware and operating systems. The three most common points of contention are whether: 1) a need to secure IT resources exists at all, 2) reasonable protection already exists due to some perceived factor, and 3) the value of expending any resources exceeds the likelihood of potential damages.

For example, earlier this year a customer declined our proposal for better firewall and system-wide intrusion detection technology. Because they *"are a small company in a non-metropolitan area, manufacturing low-tech commodity-type products,"* they believed that *"nobody but dedicated resellers would be interested in the Website, and certainly no one has anything to gain by hacking it."* Three months later, the US – Chinese "hacker war" vandalized not only their Website but also compromised their manufacturing, distribution, and financial systems through an easily exploited network connection. After we minimized the breach and restored critical IT operations, our original proposal was expeditiously approved … with additional measures.

The underlying lesson of this article: "One rarely wants to have to learn from one's own misfortune."

We cite four unique lessons to encourage IT Managers to discuss this issue with their non-IT colleagues.

Lesson One: "Perspective matters"

While small or commodity goods manufacturers inherently do not appear to constitute measurable or meaningful "targets," there is no question that any corporate Web presence can be targeted. Size, location, and type of real-world operation are irrelevant in the Internet realm, and experience demonstrates that individuals with malicious intent often choose the path of least resistance and greatest opportunity.

Lesson Two: "Mutual Relationships Produce Mutual Effects"

The tight integration of IT into corporate operations causes events affecting one area to also affect the other(s), as the Y2K problem demonstrated by threatening to shut down not only businesses and organizations but the entire computerized world. Conversely, serious events affecting an organization's infrastructure and resource levels will proportionately affect its IT operations, as would be experienced in a mandated regional evacuation due to a natural disaster, hazardous materials spill, catastrophic technological failures, or events caused by human actions.

Imagine the business fallout from a sudden business disruption. In the aftermath of September 11th, the "just-in-time" dependent automotive industry located 800 km away experienced temporary shutdowns and heavy financial losses due to cross-border parts shipment delays. An unlikely disaster directly disrupted some of the world's largest corporations.

Historically, the only recent, broad-based large-scale threat of disastrous consequence was the Y2K problem. And, since few real large-scale issues materialized, many executives quickly categorized the potential of equally large-scale disasters as highly unlikely. Only Hollywood was thought capable of creating the incredible and unthinkable.

Lesson Three: "Nothing is inconceivable … "

Regardless of our strong belief that disasters are unlikely to occur at all, or that they will not "happen to me/us," disaster-magnitude events do happen.

History is full of events once considered "unthinkable." The 1998 Montreal Ice Storm, 1996 Saguenay (flash) Flood, and 1997 Manitoba Flood, Mount St. Helens, the 1979 Mississauga train derailment, Chernobyl (1986) Three Mile Island (1977), Titanic (1912), and the 1993 L.A. Riots. Finally, any tornado, hurricane, tidal wave, earthquake, or avalanche causes a disaster when striking populated areas.

Little can be done to avert disaster-events, yet some preparedness is often the factor by which one manages to navigate them and emerge intact, wiser, even stronger. Historically, business recognized only IT Disaster Recovery plans as necessary to survive a crisis. The paradigm is now shifting away from the reactive "Disaster Recovery" (DR) and IT-only considerations to the need for a proactive enterprise-wide approach.

The events of September 11th brought this need into much clearer focus.

Because of stringent legal, audit, and reporting requirements, financial services and securities trading firms have sophisticated IT backup and DR plans. Thus, most of the firms most severely affected on September 11th had offsite backup IT systems and well-developed security plans and were somewhat prepared for a disaster. Yet, although their IT systems and data remained safe, other infrastructures and non-IT systems were not so fortunate.

The firms faced four other, more immediately severe obstacles unrelated to IT infrastructure issues:

1. Human tragedy through loss of life: Bond-trading firm Cantor-Fitzgerald was nearly decimated by the loss of 700 of its 1000 WTC staff.
2. Loss of information, and breach of security or confidentiality: documents not initially lost in fires or windblown through Manhattan's streets into parks, backyards or the ocean were finally lost in an estimated 2 million tons of rubble.
3. Inaccessibility to, or complete loss of, all operating facilities, infrastructure, and equipment: Located close to the disaster site, the American Stock Exchange's (AMEX) facilities were unusable for weeks. Its disaster plan included a backup center a few blocks away, and also arrangements with other stock exchanges for backup and crisis operations until its own facility could reopen.
4. Extreme, terrifying psychological impact of every aspect of the disaster.

Hence, despite prudent IT management, equally important 'bricks and mortar factors' were clearly overlooked, neglected, or never considered.

Lesson Four: "Broad-based, Enterprise-wide planning"

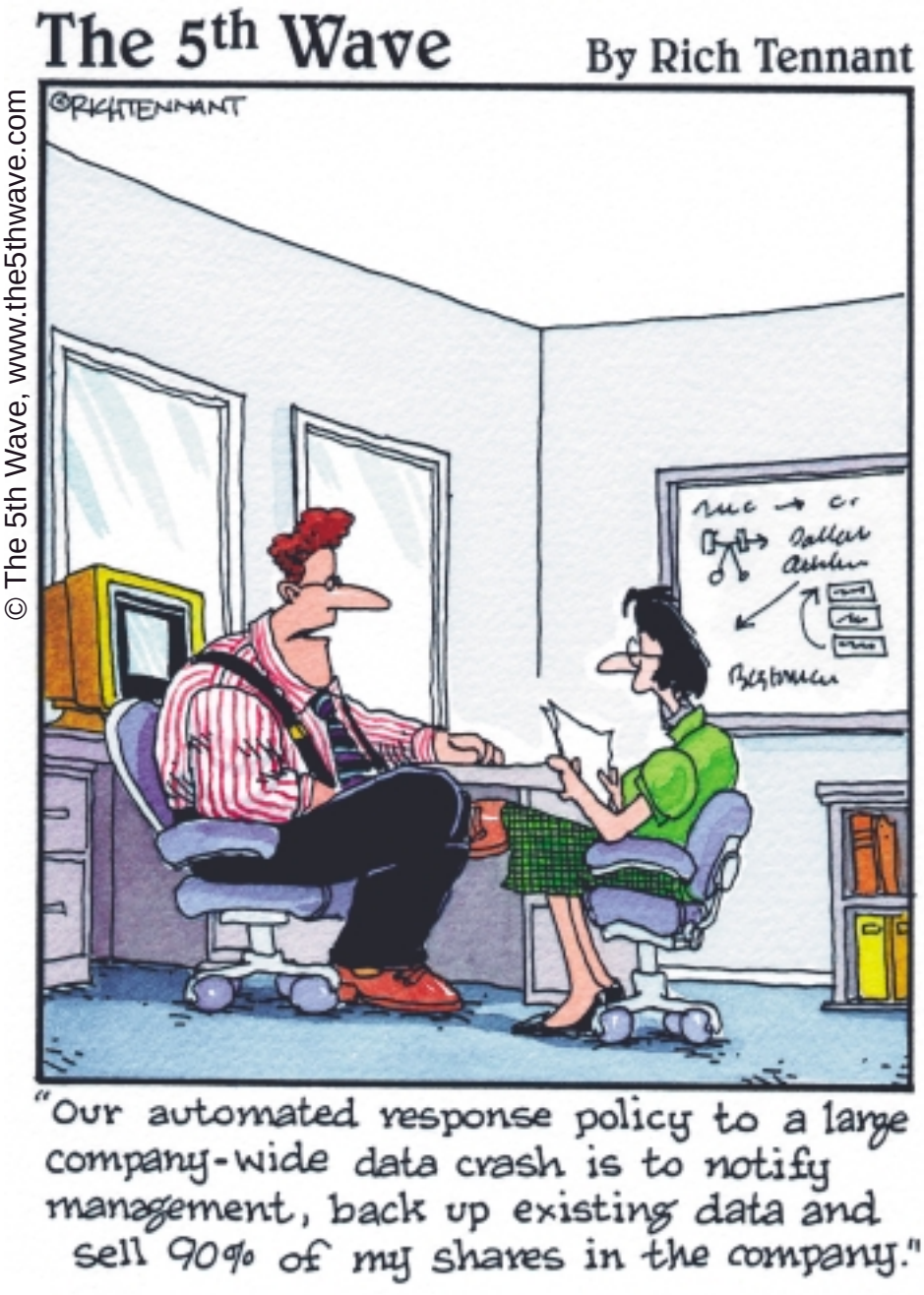
Disaster planning **must** transcend the IT function to include all business units, including sales, accounting, manufacturing, distribution, and marketing – and all their components – facilities, staff, equipment, data.

Few firms could possibly have foreseen or adequately prepared for these events, not to mention their magnitude. Each, it seems, sustained such calamitous losses that their futures could be in doubt, echoing the definition of disaster: *"a calamitous event, especially one occurring suddenly and causing great damage or hardship"* (Webster)

September 11th was certainly that, yet because many of affected businesses are financial services and securities exchange firms, all were somewhat prepared. This proved first and foremost to be their salvation, not by preventing damages, but rather by providing workable plans and crucial resources that allowed these firms to continue operating throughout the crisis, or resume shortly afterward. The fact that the attacks could have been even more disastrous must not be overlooked or forgotten.

Solution

Businesses and organizations represent substantial investments by the people they touch, the groups they interact with, and the community they operate in. Consider the sudden, broad-based, and severe nature of disastrous events that may prevent businesses or organizations from operating normally for hours, weeks or even months. Or indefinitely. The complexity of these relationships means that any major interruption among the parties will invariably impact the others throughout the chain to varying degrees.



The WTC attacks undoubtedly proved the necessity for foresight and thorough, broad-based Business Continuity Planning (BCP) that includes all operational aspects. Also apparent is the fact that no clear-cut defense exists to absolutely prevent disaster events. Statistically speaking, while the likelihood of similar events – in type or magnitude – is low, especially at this time and in our region, the possibility exists nonetheless. Therefore, those prepared for some, even minor, emergency would likely better manage to survive any type of event.

The Business Continuity Plan (BCP)

A BCP is a formal, broad-based situation anticipation, response, and action plan for "worst-case" scenarios, emergencies, and extraordinary operating conditions.

Rather than identify specific disasters or events, its purpose is to anticipate many scenarios, consider potential fallout, and mandate a range of responses or actions. Its crucial mission is to reduce the business' exposure to risk as well as the impact on its operations by providing the framework and resources for effective crisis-event management and resolution. By contrast, DR plans generally outline a methodology for restoring normal operations once a disaster has occurred; by then, though, critical failures may have already occurred.

Unlike a DR plan which only addresses point three, an effective BCP accomplishes three tasks:

- Disaster Avoidance
- Crisis/Situation Management
- Recovery to Normal Operations

While DR plans cannot inherently constitute a BCP, the latter must inherently include DR as part of its strategy. Similarly, any business should not consider itself "secure" just because its IT department follows proven policies and practices. Such organization s are at sizable risk, for example, should a large number of employees be unable to work, if a large part of its facility and/or infrastructure becomes inaccessible or is 'lost,' or when events outside the scope

or influence of the IT department prevent the business from operating effectively – or "at all." In this case, all the IT department's planning and procedures alone would not prevent heavy losses or more dire consequences.

To illustrate, any 7x24 enterprise located in Southern California would have been ill-served– as an IT strategy might dictate – by locating a critical backup or operations facility in adjacent counties, even upstate, during last summer's "rolling blackout" electricity crisis. Since similar predictions are now quietly surfacing regarding Ontario's pending deregulation of the electricity market, this is also becoming a factor for consideration.

Conclusion

Every business must have a BCP that anticipates, considers, and manages many factors, conditions, and scenarios to create a sophisticated and manageable action plan that includes multiple viable alternatives.

Effective BCP is not a simple project or document that should be undertaken in-house.

Most businesses hire lawyers, brokers, and auditors to manage legal, insurance, and financial issues. BCP undeniably falls into this grouping based on its complexity, importance, and value to the survival of the organization.

Still, IS or IT Managers can make invaluable contributions to the development of company-wide BCPs by sharing their knowledge and experiences of IT practices, disaster prevention, and recovery. Such information is critical because IT disaster policies and practices have been developed over a long period of time, and have been proven repeatedly in measurable real-world scenarios.

A comprehensive BCP can be priceless, and is best designed by independent individuals or teams that are knowledgeable about and experienced in Business Continuity Planning. BCPlanners bring to the table prior experiences and a fresh set of eyes that see various factors from other perspectives. They'll understand **your business** – not just the technology – and consider all vital aspects for its continued success. They can also manage politically sensitive ideas and make proposals without favouritism or bias.

The question an executive must ask is: *"What if….?"*

We strongly urge managers and executives in all business units to consider and discuss this with a skilled and knowledgeable Business Continuity Planning professional. Able-One Systems invites your comments and inquiries. TUG

Dave Patterson, Bio:

Dave Patterson is Senior Business Consultant at Able-One Systems Inc. With a Computer Science degree from the University of Waterloo (1973), Dave has worked in the insurance, manufacturing and distribution sectors. For the past 3 years he has been both, project manager and consultant to major health care and insurance industry clients. His most recent assignment has been to develop Business Continuity Plans for an offshore division of a global Canadian insurance company. Dave can be reached at 800-461-2253, ext. 291 or by e-mail at dpatterson@ableone.com

Dietmar Kubasta, Bio:

Between earning his Master of Arts degree from the University of Waterloo (1996) and joining Able-One Systems, Dietmar worked as a technical Sales Consultant, Communications Manager at a technology organization, as well as Business Consultant to high technology companies. As Director of Marketing at Able-One Systems Inc., his role is to help deliver the Able-One solutions teams' collective knowledge and experiences in order to assist their customers in becoming more successful. Dietmar can be reached at 800-461-2253, ext. 256 or by e-mail at dietmar@ableone.com