SIMPLICITY DATA SYSTEMS, LLC.

December 2006

Volume 11, Issue 4

SIMPLICITY IN DESIGN™

In this issue:

Special points of interest:

- Various studies show American Businesses lagging behind their European and Asian counterparts in understanding and promoting resilience.
- Misunderstanding and confusion over resilience can lead to poor planning and ineffective recovery programs.
- Different threats can be addressed using common approaches, thus reducing costs and improving opportunities to test programs and train employees.
- Culture is a key component of resilience in general and robustness in particular.

Resilience or Robustness?

This edition of ***Simplicity In Design*** focuses on systemic and cultural aspects that influence how organizations respond to major disrupting events such as natural disasters, accidents and terrorism. This subject is critically important because no matter how well we plan to mitigate threats and reduce risks, there will always be new threats and different twists on postulated threat events. In other words, chances are that highly disrupting events will challenge organizations in ways that had not been postulated. In those circumstances, organizations, that is to say employees and systems, will be forced to adapt and stretch to protect assets, personnel, operations and relationships. Specifically, the organization's ability to Compete and Perform will have to be Protected from potential long term disruptions that could undermine its competitive position.

To frame the discussion of how organizations can and should prepare to adapt to highly disruptive events, we begin by discussing the current state of enterprise resilience planning (***Resilience and American Business***) and proceed to clarify the concepts of resilience and robustness (***(Mis)Understanding Resilience***).

For enterprises with active business recovery plans and strategies, the old axiom that *No Plan Survives First Contact with the Enemy* is a truism that is equally applicable to organizations, large and small. Events that push organizations beyond postulated conditions will drive them beyond recovery, and often beyond resilience, into the realm of *robustness*. Thus, we discuss the differences between and implications of business recovery, resilience and robustness. Our last article focuses on the implications of recovery, robustness and common response opportunities, offering examples to illustrate concepts in practice.

Finally we point out that Resilience and Robustness are concepts that can and should be considered within the Protection dimension of the Compete-Protect-Perform contextual framework. This is because, ultimately, the purpose of risk mitigation, business recovery, organizational resilience and robustness is to protect a business' ability to Compete and Perform *before and after* a disrupting event.

We urge to contribute your inputs on these topics by phone or via simply@simplicitydata.com.

Resilience and American Business

American businesses rank well behind their Asian and European counterparts in understanding and promoting enterprise resilience. This is the conclusion of the US Council of Competitiveness, an organization formed in 1986 to provide a "*forum for elevating national competitiveness to the forefront of national consciousness.*"

In ***Enterprise Resilience***, a summary paper, the Council points out that:

(1) Only 36% of US CEOs believe that risk management is a priority concern versus 45% of their European and

Continues on Page 2

(*Mis*)Understanding Resilience

Resilience is conceptually simple but difficult to pin down in practice. Programmatically it is often confused with business recovery in part due to its informal definition as '*an organization's ability to gracefully recover from a disrupting event.*' To succeed programmatically, resilience has to transition from concept to practice, which entails the development of formal terminology, methodologies and performance metrics.

Defining Resilience

From an engineering perspective, systems are designed to operate within specified requirements, which together define their operational envelop. All engineered systems, however, are also designed to operate outside normal parameters in response to perturbations and disruptions. This extra performance margin is intended to ensure adaptability and reliability under 'real-world' operating conditions.

Systems are also generally designed to fail in predictable ways so as to avoid catastrophic damage and facilitate recovery. For example, an electric fuse or circuit breaker is a common method of disrupting electric power to a system drawing excessive current. Thus, if a motor is placed under increasing load, it will eventually draw too much current causing the circuit breaker to trip. Motors are designed to absorb excessive loading for a period of time, so the breaker or fuse will effectively protect it from damage.

In general, designed resilience seeks to define a competence model with boundary conditions within which the system will either adapt to perturbations and continue to function or fail gracefully, so that operations can be quickly restored.

Beyond designed resilience lies an area of increasing importance, particularly in highly complex technical and social systems. It involves preparing the organization to survive events that cause upsets and disruptions outside predicted/designed for factors. We call this aspect of organizational adaptation beyond designed resilience '*robustness.*' The opposite of '*robustness*' is fragility or brittleness, which denote the inability of a system or organization to adapt to stressful conditions outside of its designed *resilience envelop.*

A Few Examples

Aloha Airlines Flight 243

On April 28, 1988 Flight 243 experienced explosive decom-

Continues on Page 4

Resilience is a conceptually easy and operationally difficult process to implement. It is often confused with business recovery and a sense of the robustness of organizations, systems, equipment, people, etc.

Resilience and American Business (Continued from Page 1)

65% of their Asian counterparts.

(2) Only 25% of Directors of non-financial companies report that the Board considers all major risks to the company, versus 55% of industry directors.

(3) During the past twelve months (2005-2006), twenty percent of companies surveyed by The Economist suffered significant damage from a failure to manage risk and over half had been at risk of such an event.

They also point out that hundreds of large companies over the past ten years have suffered supply chain disruptions resulting in 33-40% lower stock returns than their industry peers. Major disruptions in supply chains have caused companies significant market share that in some cases resulted in permanent loss of market leadership. In some cases, disruptions have been triggered by manufacturer production and quality problems caused by poorly executed off-shoring plans.

Improving operational resilience requires a thorough understanding of the functions, assets and players, internal and external, on which enterprises rely to deliver their products and services to market. It also requires a thorough understanding of evolving threats and their implications. So far, American CEOs remain divided over the need to invest more and pay greater attention to the inherent resilience of their enterprises. Only time will tell if their thinking is proven to be sound or short sighted.

Supporting Evidence:

Simplicity Data Systems and AC Macris Consultants have been conducting a survey of industry attitudes towards terrorism. Preliminary data from the survey supports the findings discussed in Resilience and American Business.

Implications
Different Threats—Common Options

Recovering from most threat events is a process that involves returning people, systems and facilities to operation. While sometimes operations can be relocated or consolidated in undamaged facilities, in most cases, recovery involves salvaging, repairing and replacing assets 'in situ'.

Operational aspects such as the need to operate near specific fixed assets, retain access to employees and remain accessible to its local client base can tightly bind company operations to specific geographic areas. This is also the case for much of the national critical infrastructure including water, gas and electric utilities, telecommunications, agriculture, banking and finance, transportation, health and government services.

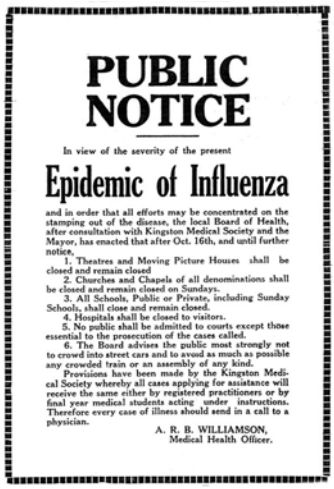
Even when operations are ultimately relocated, the process will likely require access to affected sites in order to recover records, move equipment and salvage materials. In many cases, companies will be working to recover operations before reaching their Maximum Tolerable Downtime, the point at which they become essentially unrecoverable. Even when Business Disruption Insurance can temporarily offset revenue losses, it will only reduce their short term impacts, not replace what was and will ultimately be lost.

Some Threats Can Be More Threatening than Others

Threat events have unique characteristics that can affect recovery efforts. Two key factors are the event's impacts on the workforce and access to facilities/assets. To illustrate this relationship, we will consider two specific threat events: Pandemics and Radioactive Dirty Bombs.

Pandemics

Pandemics have been with us throughout history and history clearly documents the severity of their impacts. The Black Plague, Small Pox, Cholera and Influenza have at times decimated societies and altered entire social and political systems. In the twentieth century, the deadliest pandemic was the Spanish Flu of 1918—1919, which killed an estimated 50 to 100 million people worldwide. The killer was a virulent strain of the H1N1 Influenza A virus, which took advantage of increased human mobility and war (WWI) to propagate from North America to Europe and beyond.



PUBLIC NOTICE

In view of the severity of the present

Epidemic of Influenza

and in order that all efforts may be concentrated on the stamping out of the disease, the local Board of Health, after consultation with Kingston Medical Society and the Mayor, has enacted that after Oct. 16th, and until further notice,

1. Theatres and Moving Picture Houses shall be closed and remain closed
2. Churches and Chapels of all denominations shall be closed and remain closed on Sundays.
3. All Schools, Public or Private, including Sunday Schools, shall close and remain closed.
4. Hospitals shall be closed to visitors.
5. No public shall be admitted to courts except those essential to the prosecution of the cases called.
6. The Board advises the public most strongly not to crowd into street cars and to avoid as much as possible any crowded train or an assembly of any kind.

Provisions have been made by the Kingston Medical Society whereby all cases applying for assistance will receive the same either by registered practitioners or by final year medical students acting under instructions. Therefore every case of illness should send in a call to a physician.

A. R. B. WILLIAMSON,
Medical Health Officer.

International consensus at this time is that the threat of another flu pandemic is on the rise. The threat is considered sufficiently severe that the US government is investing billions to prepare the nation. Historically, influenza pandemics involve multiple outbreaks extending over the course of two seasons (1918-19, 1957-58 and 1968-69).

An influenza pandemic's primary impact on business operations will be felt through the interconnecting human chains in modern economies (employees, customers, partners and suppliers). Local companies whose workforce is severely affected will likely have to ride out the event in an environment where services such as food and health are severely strained.

Larger companies with geographically dispersed operations may be counting on shifting employees to temporarily augment their workforce in affected areas. This strategy is only practical when employees brought in from unaffected areas are vaccinated and willing to risk exposure to the virus. At best, this scenario is fraught with risks since many employees may refuse to enter areas affected by the flu. Local, State and Federal authorities will also limit travel to affected areas as a containment measure. Thus, operationally, a key challenge facing enterprises will be to ensure that they can continue to operate with a severely diminished local work force.

Nuclear Terrorism

Nuclear terrorism is most likely to involve the use of a dirty bomb. A dirty bomb is a device composed of an explosive core surrounded by highly radioactive material. The explosion would fracture and spread the radioactive material directly from the force of the explosion and indirectly in the form of airborne particle

Continues on Page 5

When different threats are considered in light of their common impacts and mitigation alternatives, options emerge for improving resilience at reduced costs.

(*Mis*)Understanding Resilience *(from page 2)*

pression during flight, which ripped portions of the top of the main cabin, throwing a flight attendant to her death and injuring most of the remaining passengers and crew.

In spite of extensive damage, as illustrated in the image, Captain Robert Schornsteimer and First Officer Madeline Tompkins managed to retain control of the aircraft, declare an emergency and safely land the Boeing 737-200 without additional injuries or loss of life. The only fatality was that of flight attendant Clarabelle Lansing, who was standing in the center aisle when the incident occurred.

In this case, the airframe and flight systems managed to survive a catastrophic failure and the air crew effectively responded to the event in time to avoid a complete catastrophe. Thus, both engineered and social systems effectively adapted to an event outside designed resilience boundaries. Boeing's reputation for building safe, robust aircraft and the training, experience and adaptability of the aircrew demonstrated the robustness of the industry across corporate boundaries.

Fickle Acts of Nature

Nature's wrath was in full view in 2005 and 2006, as hurricanes and tsunamis brought massive devastation to geographically distant US Gulf Coast and Pacific nations. In the US, corporations such as Home Depot and WalMart received extensive positive coverage for their ability to quickly reopen stores and deliver much needed supplies to the most affected areas.

4-26-1988 After 89,090 flight cycles on a 737-200, metal fatigue lets the top go in flight.

Operating in the midst of devastation is one way in which organizations demonstrate their robustness. In every case, achieving this level of resilience involves both systems and people. During the November 2006 OSAC meeting at the US State Department, two of Target Stores' risks managers delivered a presentation on the company's approach to restoring store operations in the aftermath of a major disruptive event. Target's strategy includes preparation, post event assessment and employee support.

For example, before a storm hits, store managers secure their facilities and validate employee contact information; after the event they quickly assess the damage to their facilities and contact employees to establish who is available to work. Corporate risk managers remain in contact with affected store managers, directing additional resources where they are needed most. At the employee level, payroll has to be met and this may require disbursement of cash payments in areas where banking services are disrupted by the event.

Quantifying Robustness

Robustness is about organizational adaptability to disruptions that exceed the boundaries of engineered resilience. This can happen when changing operational realities are not identified, assessed and incorporated into the organization's impact mitigation and recovery programs. Consistently monitoring and adjusting to changes in the organization's operational environment are key to keeping business recovery planning up to date.

Organizational robustness is also tested when low probability-high impact disruptions occur, which were not accounted for within the organization's recovery plans. There are no right or wrong answers when it comes to prioritizing and incorporating specific threats into recovery plans. Each organization has its own risk tolerance threshold and will respond positively to address related impacts or spread the risks through a variety of insurance vehicles designed to reduce associated financial burdens.

In the end, maximizing robustness requires the organizational ability to extend systems and people beyond their designed margins, preparations and training. While conceptually this is simple to illustrate, quantifying it is another matter.

Since robustness by definition defines an area not covered by engineered resilience, it remains a qualitative as opposed to a quantitative aspect, at the intersection of systems and culture. Thus, to a large degree, robustness is dependent on people and culture, both of which can be affected through training, management and leadership development. This will be the topic of a future article. Stay tuned!

Robustness cannot be fully quantified because it occupies a space beyond planned recovery and Resilience. It can, however, be demonstrated, promoted and qualitatively described.

Implications
Different Threats—Common Options *(from page 3)*

deposition.

While a dirty bomb will not cause widespread illness, it is likely to contaminate large areas, delaying for days, months and potentially years enterprise recovery operations. Thus, even if facilities, equipment and materials are not damaged by the explosion, they may remain unreachable and ultimately unusable based on the actual, potential or perceived danger of contamination.

The workforce will also be affected through fear, displacement and employment uncertainties. Unlike pandemics, which are likely to last six to eight weeks, radioactive contamination may take years to remediate. Thus, relocation may ultimately become the only practical recovery option for jobs and inhabitants alike.

Common Response Options

While pandemics and nuclear terrorism are significantly different threats, mitigation strategies can still share methods and resources. These include telecommuting, geographically dispersed backup of key functions and information, compatible methods/processes across common operations in geographically dispersed facilities and organizational culture hardening.

When recovery strategies and methods are shared across postulated threat events, enterprises can benefit from lower business recovery program costs, greater simplicity and improved response. More importantly, by developing a culture that seeks to adapt common response strategies, capabilities and methods to varied recovery scenarios, organizations promote creativity, analysis and agility in the face of challenging and often deteriorating conditions, i.e. robustness.

From Resistance to Robustness

Resilience is a reflection of an organization's ability to gracefully recover from disrupting events. For the most part, this is a capability that cannot be fully demonstrated. Why? Because, we are limited in our ability to predict all possible or even likely threat events and their actual impacts. Similarly, we cannot fully predict how organizations will respond to sudden shifts from normal to response-recovery operations, while under high stress.

For example, some threats can be identified in time to prepare the organization to respond. These include hurricanes and other developing weather patters, pandemics and worsening political conditions. The hurricanes that ravaged the US' Gulf Coast in 2005 granted companies such as WalMart and Home Depot the opportunity to prepare pre-event to effectively respond post-event. In these cases, emergency procedures were triggered before the fact and entire logistic chains adjusted to maximize post event operations.

Most of the time, however, organizations will get little or no warning. On 9/11, organizations operating out of the World Trade Center faced the complete destruction of their assets and in some cases much of their intellectual capital. One example that has come to epitomize culture and attitude in recovering from one of the greatest disasters to befall an organization is the trading company Cantor Fitzgerald (CF). On 9/11, CF lost every employee who was at their WTC desk, a total of 658. The one surviving executive partner and current CF CEO, Howard Ludnick, described in an interview to Business Week what it felt like in the aftermath: "*I'd tell people it was like I was surfing in front of a very large wave and as long as I kept going forward as fast as I possibly could, the wave would never get me. But, if I ever stopped, and took a moment to look back … Whoosh, the wave would crash over me and I'd get crushed. But, if I kept moving forward, the wave would get smaller and smaller.*" According to Business Week, "*Survivors are quick to share stories of 90 hour weeks, of adrenaline-fueled problem solving, and of an unshakable belief in one another. Work was not just a distraction; most say it healed them*". It took CF over four years of intense effort to recover from a single catastrophic event, but the point is that CF did recover.

CF had good information backup processes that made business recovery possible. By all measures, CF was, from a systems perspective, resilient. Ultimately, however, it was their robustness that was tested given the magnitude of the event and it was their culture, from executive to the 'factory floor' that made recovery possible.

This article was authored in collaboration with Dean Macris of AC Macris Consultants.

Many threat events quickly overwhelm planned responses and recovery scenarios. At that point, it is the organization's robustness in general and culture in particular that will be tested.

Responding to different threats with shared resources and methods.

SIMPLICITY DATA SYSTEMS, LLC.

PO Box 57
Loveland, CO 80537
www.simplicitydata.com

Phone: 970-213-1550
Email: simply@simplicitydata.com

SIMPLICITY DATA SYSTEMS, INC.

THE MOST COMPLEX PROBLEMS ARE FREQUENTLY SIMPLY SOLVED

Simplicity Data Systems is an applied research, business consulting and strategic analysis organization. Its focus is on evolving business models and the protection of the US homeland/economy from terrorism and other disrupting events. Over the past six years, SDS has focused on global threats from pandemics, conflicts and terrorism, while concurrently developing new business, threat assessment, risk mitigation and resilience models.

Our work is reflected in our writing, which is accessible from the Published page of our web site: *www.simplicitydata.com*.

Summary Points and Takeaways

Understand the differences between business recovery, resilience and robustness:

- Business recovery is an aspect of resilience,
- Resilience should be thought of as the designed capabilities of an organization or system to stretch beyond normal operating conditions and gracefully recover from disrupting events,
- Robustness refers to the organization's ability to adapt and recover from disrupting events for which no designed/validated recovery capabilities are in place,
- Robustness cannot be proven on paper. It can only be demonstrated in how organizations respond to disruptions and unexpected operational conditions,
- The less prepared a company is to recover from postulated disrupting events, the more its robustness will be tested by such an event,
- There is nothing left beyond robustness. If robustness fails the organization will cease to exist,
- Culture is a key component of organizational resilience in general and robustness in particular. Disrupting events cannot be fully described and prepared for and often occur without warning. At that point, organizational response will generally reflect its culture, from the executive level to the 'factory floor,
- Organizational culture can be hardened to strengthen resilience and promote robustness.

Please contact us to contribute your thoughts and comments, ask questions or request additional information on our research focus and related services. Send e-mails to: ozzie@simplicitydata.com

References

For a discussion of Resilience see the Council on Competitiveness report on The Value of Resilience.

For discussions on robustness, consult the Santa Fe Institute's Robustness Site.

For the Business Week article on Cantor Fitzgerald see 9/11 Five Years Later—A Tale of Renewal.

For a discussion of the impact of a Radiological Dirty Bomb see the report by The Federation of American Scientists.

For a discussion of the impact, assessment and preparations for future pandemics, see the Federal Government sponsor site on Pandemic and Avian Flu.