

Real Estate Strategies

You Can Never Be Too Prepared

BY MARTIN LEVY, CEO
ITRA / MARTIN LEVY COMMERCIAL, LONDON

IT TOOK A FIRE AT MY OFFICE FOR THE LITTLE LIGHT TO GO ON. JUST HOW VULNERABLE IS EVERY BUSINESS, REGARDLESS OF SIZE, TO DISASTER? DO WE REALISE HOW MUCH WE LEAVE BEHIND EACH NIGHT WHEN THE LIGHTS GO OFF?

Consider that:

- 43% of companies suffering a disaster never recover
- 80% of companies without a Business Continuity Plan fail within 18 months of a disaster
- It is estimated that 90% of hackups will FAIL to restore data as required*

**(A Guide to Business Continuity Planning”
Chelmsford Borough Council, UK)*

It doesn't matter how big or small your company is, or whether you have teams of executives or consultants involved in disaster preparedness. The simple truth is that being prepared to survive the unexpected requires constant vigilance.

Unless we constantly review, revise and test our procedures and systems, adjusting to new and changing threats and circumstances, we may not be prepared for disaster.

Complacency leaves us vulnerable to disaster. Consider that ten years ago, global computer “worms” were not as common or lethal as today. The 9-11 attack in the US had not yet happened. How inconceivable was the terrorist attack in Mumbai, assisted by VOIP technology and



remote communications with real time instructions? Could anyone have envisioned global pandemic biological threats or the Katrina disaster in New Orleans?

Times change. Threats change.

As the world changes, those planning to protect their companies against disaster must be prepared to change their thinking, preparations and approaches.

A good starting point for all companies, large and small is the Risk Assessment Matrix (RAM) created by The School of Criminal Justice of Michigan State University. RAM is a template for a thorough, scheduled periodic review of your firm's disaster preparedness. Large

corporations and major government agencies have similar comprehensive checklists, and there are firms specializing in disaster recovery that focus on such specific aspects as computers or telephony.

Every business should start with core functions and processes:

- Communications
- Customer service
- Facility management
- Human resources
- Information technology
- Inventory
- Marketing and Sales
- Production
- Shipping/receiving
- Training

Make a list of all of the conceivable threats, ranging from such natural occurrences as **storms, earthquakes and floods**, to man made situations such as **terrorist strikes, biological disasters, explosions, technological interruptions, civil disturbances** and the **loss of a key customer or supplier**.

Using a spreadsheet, the review should identify *critical* areas, as in what is necessary or a safety risk. This should be distinguished from what is *essential*, as in what might become critical in time versus what may be *inconvenient* or *non-essential*. Each business function should be labeled according to its likelihood and vulnerability to being affected by these threats.

For each contingency, a plan of action should be prepared. What is the plan in the event of a plant closing, hazardous materials discovery, fire evacuation, etc? What preparations have been made for vital records protection, mutual aid agreements or shelter-in-place?

Is there a hierarchy for emergency responses? If the CEO is not available, for example, who authorizes an evacuation order? What is the emergency response plan? Is an emergency management group needed? Are the emergency responders identified, regularly trained and equipped? What are the protocols for releasing information to the public?

Facilities and equipment issues must be included in disaster preparedness. This covers emergency facilities as first-aid stations, emergency operating areas, media briefing area, shelters, etc. Equipment might include fire

protection/suppression equipment, warning systems, first aid supplies, emergency power generators, communications equipment and decontamination equipment.

With all of these serious disaster preparedness issues to address, there's still one area that can be easily forgotten, but is nonetheless quite critical: the lease(s) under the company's control. A property lease should be written providing for some tenant protection. (This is more likely to happen when working with an unconflicted tenant representative, like an ITRA exclusive tenant representative).

In the lease there needs to be clear definitions about what happens when a tenant cannot occupy a space. Under what conditions is a company obligated to pay rent to the landlord when the space is only partially habitable?

When negotiating a lease, a tenant should try to determine who (tenant or landlord) bears the risks in specific situations and who pays for and provides the insurance coverage. For example, the Fire and Casualty provision may indicate that if the tenant is unable to utilize the premises due to casualty, the tenant does not pay rent until the repairs are made.

If your firm faces a disaster, it may be forced to relocate and pay for higher than the existing rent. Business Interruption Insurance covers lost income, and Extra Expense Insurance, which covers additional rent and expenses. This should be considered a part of your disaster preparedness and business continuity strategy.

Companies preparing for a possible disaster must not only consider every contingency that affects their office space and physical assets, but also what happens if and when they become separated from their space during an emergency.

It's not just good business—it's a matter of survival!

(Martin Levy may be reached at mlevy@itraglobal.com)