

Emergency Preparedness

What keeps you awake at night? Do you worry about meeting analysts' expectations? Launching a new product on time? Traveling overseas when a conflict or epidemic breaks out? Coping if a flood, fire, earthquake, or tornado affects one of your facilities or one of your key suppliers?

An emergency preparedness plan won't help you make strategic or product decisions, but having contingency plans in place to deal with emergencies – before they happen – can help you rest a little easier. In fact, thanks to solid contingency plans, a computer consulting firm based in New York City barely missed a beat after one of the worst terrorist attacks ever on U.S. soil.

Located within blocks of the World Trade Center, the company was shut out of its building for almost three months after 9/11. But because there was a plan to follow in case of a catastrophic event, they were able to re-establish operations from remote locations across the general metropolitan area – and fully resume services for their clients – within four days!

How did they accomplish this – when so many other firms failed? Two words – advance planning. One of the company's top priorities was to make sure there were procedures in place not only for daily backups of all data, but also for storing these backups off site – and making sure they were easily retrievable.

In addition, they had made arrangements to secure temporary office space, furniture and utilities. They also had planned how to keep their employees working if their normal offices were unavailable. So, when the disaster occurred, they didn't have to negotiate for space at a time when so many others in downtown Manhattan were doing the same thing. Their plan worked and they were able to limit what could easily have been a multi-million dollar loss to just \$600,000!

Plan for the Most Likely and Most Costly

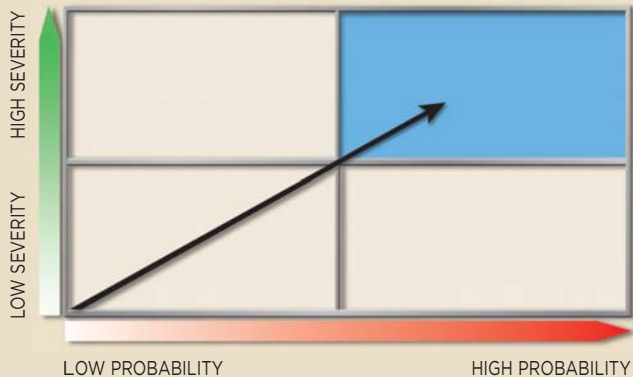
If you don't think you can plan for every single emergency... you're absolutely right! You can, however, assess potential hazards that pose a real threat to your business. First, determine what those threats might be. Think about the obvious ones such as fire or flood, as well as the less obvious ones such as theft of key equipment. Of course, depending on your firm's specific operations, location, and workforce, you may be exposed to any number of other significant risks, including:

- Accident with hazardous materials
- Cyber crime
- Interruption in the supply of materials
- Loss of a key employee
- Loss of original documents
- Natural disaster such as:
 - Fire
 - Flood
 - Earthquake
- Power failure
- Sabotage
- Severe medical emergency
- Terrorism
- Theft of computers
- Workplace violence

Then, evaluate which of the risks you've identified have the highest probability of occurring. Once you've compiled your list, you'll want to analyze which one(s) could take the greatest toll on your business. Focus your emergency preparedness planning on managing the risks with the highest probability of occurrence and the biggest potential impact on your business.

How to Analyze Your Firm's Potential Risks

Since you simply can't plan for every type of risk that may occur, use this grid to categorize which would be the most likely – and the most severe – if they did occur. Then focus your emergency planning efforts on those risks.



Pay Attention to the Fundamentals First

Events such as tornadoes, floods, terrorist attacks, and workplace violence get everyone's attention. Fact is, the majority of technology firms never experience these types of disasters. While your emergency plans should address these possibilities, you should also be aware of, and develop plans, to address more routine exposures to prevent them from becoming business catastrophes. Think about these examples of potential "catastrophes":

- You arrive for business one morning only to discover that one of your servers – mistaken for just another computer – has been stolen. While most people wouldn't describe computer theft as a "catastrophe," for a technology company, the loss of the wrong computer at the wrong time could severely disrupt your business – and cost you in terms of lost contracts or customers. Implementing premises security, reference checks on all employees and new hires, and other very basic techniques may be all you need to protect your business from the routine causes of business emergencies such as theft.
- Your power supply goes out for 10 minutes, an hour, a day or worse. It's not a pretty picture. As companies on the West Coast are already painfully aware, a power outage can disrupt business. And yet, many companies take the availability of power for granted.

This can be a huge mistake. Taking a few simple precautions such as using an uninterruptible power supply and having back-up generators can help protect your business from unnecessary interruption.

Here are some additional tips that can help you prevent something routine from becoming catastrophic.

- **Keep critical pieces of technology, such as servers, hubs, routers and phone systems in locked areas of your office.** Limit access to only a few people, and require them to use pass codes.
- **Record serial numbers.** Make sure the serial numbers for all hardware (and software) are recorded and stored in a safe place, preferably off site. This way if your equipment is stolen – and then found – it can be easily identified as your property.
- **Locate all of your company's crucial data files, including any confidential files on laptops and PCs.** Make sure they're backed up, tested, verified and checked on a regular basis.
- **Store all backup files off site.** Make sure your off site storage facility has security measures in place for their backups to guard against tampering, theft or disaster.
- **Minimize inventory.** Keep only what you need on hand. Store extra equipment in a secured facility off site. And make sure to do regular – and surprise – counts of what's in storage.
- **Install anti-virus software, load balancing technology and firewall protection on all of your company's computers to guard against cyber crime.** Also, use passwords to prevent unauthorized access and tampering.
- **Implement an active server monitoring program that notifies you anytime your connectivity is down.**
- **Don't depend on a single source for raw materials and supplies.** Arrange for alternative sources. And diversify geographically. This way if a disaster affects one part of the world, you've got a source somewhere else.
- **Identify ways to span an interruption of supply –** especially for rare materials and hard-to-find hardware and software. Negotiate contractual agreements up front with suppliers or mutual use arrangements with nearby companies that use the same equipment.

For More Information

For more information on how to manage risks for your business, contact your local Hartford agent, or visit www.thehartford.com.

Best Practices for Your Business

About The Hartford's Technology Practice Group

For more than 25 years, The Hartford has insured technology and life science businesses of all sizes. Our products are flexible enough to grow with a business – from a startup or sole proprietorship to a large, publicly traded company. We also offer services that can help businesses lower their losses, like our series of Technology Best Practices.

The information provided in these materials is intended to be general and advisory in nature. It shall not be considered legal advice. The Hartford does not warrant that the implementation of any view or recommendation contained herein will: (i) result in the elimination of any unsafe conditions at your business locations or with respect to your business operations; or (ii) will be an appropriate legal or business practice. The Hartford assumes no responsibility for the control or correction of hazards or legal compliance with respect to your practices, and the views and recommendations contained herein shall not constitute or undertaking, on your behalf or for the benefits of others, to determine or warrant that your business premises, locations or operations are safe or healthful, or are in compliance with any law, rule or regulation. Readers seeking to resolve specific safety, legal or business issues or concerns related to the information provided in these materials should consult their safety consultant, attorney or business advisors. All information and representations herein are as of January 2010.

