



A White Paper from

 **Techcare**™

Protecting Your Business from the Unexpected

How Bad Will it Hurt?
How Long Will it Last?

Authored by:
Steve Feldman
Techcare, LLC President

ABOUT THE AUTHOR

In 1987, Steve left his career as a CPA to take the “easy” road of starting a networking VAR. Steve, his partners and staff have worked to grow Techcare to be a successful and profitable company serving Small Business Professional Service Firms and various niche markets in the Chicago area, including the Creative and K-12 Education markets.

Techcare has been a top performer in industry peer groups, and is actively investing to address customer needs in the area of Managed Technology Support Services. Steve has participated in various industry and vertical market affiliations, including representing Venture Tech members on the VTN U.S. Advisory Council. Steve has been a speaker at various industry trade shows for the small business, Graphic Arts and Education industries.



Protecting Your Business from the Unexpected

White Paper Discussion

Protecting your Business from the Unexpected

How Bad Will it Hurt?

How Long Will it Last?

"In our 24/7 world where even our kids are hyper-connected, a few hours of technology downtime will usually prove costly."

Overview and Position

One would think that with all the improvements in technology over the last 20 years, things would just "work" all the time. But even in the futuristic world of Star Trek, Captain Kirk's "Chief Tech Guy" Scotty had been quoted saying "Aye sir, the more they over-tech the plumbing, the easier it is to stop up the drain."

In the real world that makes up your business technology, things seem to be getting more complex – not simpler. Microsoft, Cisco, SPAM, Apple, Adobe, Blackberry – on and on.

Your firewall needs to communicate with your server, so that your VPN talks to your printer, so a hacker won't access your laptop while you drink coffee at a local coffee-shop, and you hope your email system does not stop sending mail to your clients.

Let's face it. Today, business and IT risks *ARE* closely intertwined. In our 24/7 world where even our kids are hyper-connected, a few hours of technology downtime will usually prove costly. And in many cases, any really significant downtime could be considered a true business disaster.

"70% of business people have experienced some sort of information technology data loss"

If It Can Happen - It Will To Someone!

If I had a dollar for every time a client told me that something bad won't happen to them... well, you know the rest of that one. According to the National Archives and Records Administration in Washington, 70% of business people have experienced some sort of information technology data loss. Also, more than 90% of businesses that lost access to their data and their data-center for 10 days or more *filed for bankruptcy within 1 year!*

What You Don't Know Can Hurt You!

Do you know if your business technology systems are generally Disaster Tolerant? Rank yourself before reading on (see next page).

If you scored at least 45, you likely have a Disaster Tolerant IT environment. If not, you should definitely read on!



Protecting Your Business from the Unexpected

5 for a definite YES, 0 for NO (or if you do not know)

How do you rank on...?

RANKING

- 1. Our executive team has a clear understanding of key decisions about the technology we install and how we secure it..... _____
 - 2. I know what data information in my business is being backed-up, how often it is backed-up, and that the back-ups are tested and are accessible in an emergency..... _____
 - 3. We know how much downtime we can sustain before a business crisis occurs, AND we know that our systems are set up to not fail beyond that downtime expectation..... _____
 - 4. If our servers/network undergo a significant outage, our staff knows what to do to get things back up and running within the specified timeline, and the plan is documented _____
 - 5. If my (or other key executive's) laptop or cell phone is lost or stolen, our data network is safe and secure..... _____
 - 6. When an employee leaves us, our process for securing their access to information is solid..... _____
 - 7. If our building is not accessible we have a plan in place to continue operations of key systems, and can access our applications, email, and data..... _____
 - 8. Our network is secure from the outside _____
 - 9. Our systems are centrally managed, tested and validated by Spyware and Virus protection, and it is automated _____
 - 10. Our technology systems are well documented and this information is in a secure location..... _____
- ADD UP YOUR SCORE: (0 TO 50)** _____



Protecting Your Business from the Unexpected

“Knowing what risks may exist (as well as how likely they may be to occur) is an important step in determining how exposed a business’s IT assets are.”

Are You Exposed?

Likely or not, risk exists. Many businesses today are realizing the important role technology plays in daily activities, maybe even understanding the real impact that an unplanned information loss or technology outage can have on the business.

However, relatively few businesses have developed plans to quickly recover from a technology-robbing disaster.

Threats may come from outside a business. Is someone hacking into the network? Would you even know? A hacker may be a vandal interested in criminal mischief or a competitor looking for an illegal advantage. All of these risks must be considered, especially since e-commerce has opened up our networks to customers, vendors, and others over the Internet.

Sometimes, the risk is internal. Statistics show that half of all network intrusions come from the inside—behind the firewall designed to protect you from hackers. These may be “trial hacks” by disgruntled employees or the honest mistakes of a user with the wrong security profile. Regardless of intent, the damage can be real. The news is flooded with stories about disastrous events every day. But rarely do they share the information technology implications of these events:

- Hurricanes
- Electrical storms
- Criminal acts
- Auto accidents
- Virus attacks
- Loss of power
- Flooding
- Tornados
- Staff dishonesty
- Fires
- Explosions
- Chemical spills

Knowing what risks may exist (as well as how likely they may be to occur) is an important step in determining how exposed a business’s IT assets are. But a business owner also needs to know how much such a crisis will “hurt” and how much “pain” the business can sustain.



Protecting Your Business from the Unexpected

How Much Will It Hurt?

(Business impact or consequences)

In reviewing Disaster Tolerance, one must ask "If something happens, how bad will it hurt, and how long can we deal with this level of pain?" In doing this, priorities start to emerge that allows one to:

1. Identify the impact of threats
2. Identify most critical areas and prioritizes them
3. Determine how long the organization can "go without" a specific function(s):
 - a. Core process – Mission critical
 - b. Support process – Minimum activity to support core process
 - c. Discretionary process
4. Determines how much it will cost for the downtime.
5. Determines legal and regulatory obligations should a disaster occur.

"I hear business owners say time and again that no downtime is acceptable. However, when the cost to create a Zerodowntime environment is shared, a lesser expectation is usually the result."

Knowing how much an outage will hurt leads to the next question: "What is the maximum tolerable downtime?"

I hear business owners say time and again that no downtime is acceptable. However, when the cost to create a Zerodowntime environment is shared, a lesser expectation is usually the result.



Protecting Your Business from the Unexpected

“At some point, a business needs to determine how best to shift the risks.”

Making It Better ***(Risk Shifting)***

Up until now, this report has been focused on determining what to protect, what to protect it from, and how much protection is needed. At some point, a business needs to determine how best to shift the risks.

Safeguards can be applied to reduce risks. They can either be proactive (protecting the technology asset before there is an incident) or reactive (protecting the asset when an incident is detected or occurs). Safeguards reduce risks through one or more of the following methods:

Avoidance. A proactive safeguard intent on keeping incidents from occurring and is the preferred method. Incidents can be avoided by employing a number of processes, including:

- Reduction of threats with better systems
- Removing vulnerabilities with better design
- Limiting access to important resources

Transference. Allows an organization to limit losses to a predefined and predictable amount based on legal contracts. Transference shifts the risk to another organization, and includes:

- Insurance.
- Outsourcing

Mitigation. The process of minimizing the impact of an incident. Key elements of mitigation include:

- Improved detection.
- Rapid response.

Acceptance. If the risk is small enough, an organization can choose to ignore it.



Protecting Your Business from the Unexpected

“Instead of reacting in the hazy hours following an actual disaster, a plan identifies where unnecessary exposure to risks exist and allows for proper cost/benefit-based decisions.”

Protecting a Business With a Plan

Why Plan?

A documented disaster recovery plan allows one to understand which assets are vulnerable along with recovery priorities. Instead of reacting in the hazy hours following an actual disaster, a plan identifies where unnecessary exposure to risks exist and allows for proper cost/benefit-based decisions.

A plan should answer the following questions:

1. What is the likelihood that this will happen?
2. What aspects of my business will it affect?
3. What is my overall business strategy to deal with it until life gets back to normal?
4. Who are the critical people needed to keep the business running?
5. What are my back-up resources and are they ready to deploy?
6. What are the outlined procedures I need to take during the crisis?

The result of a plan should be:

1. Planning for and preventing business interruptions
2. The ability to continue your critical business functions during and immediately after a disaster
3. The restoration of your business to pre-disaster conditions



Protecting Your Business from the Unexpected

Some Words of Wisdom when thinking about a Disaster Recovery Plan -

"In the event of a crisis, whether an attack of man or of Mother Nature, it's critical that our response as a country be quick, coordinated, and comprehensive."

*Former Department Of Homeland Security Director
Tom Ridge*

"Plan for a recovery that addresses everything from computers to customer service phones to paper-based assets."

"Knowledge is going to make you stronger. Knowledge is going to let you control your life. Knowledge is going to give you the wisdom to teach their children. Knowledge is the thing that makes you smile in the face of disaster."

Avery Brooks

"D'oh!"

Homer J. Simpson

Ten Tips For Success

<http://www.infosec.uga.edu/bcpdrp/tentips.php>

- **Prepare for the Worst.** Imagine worst-case scenarios when planning for disasters. Don't underestimate any single difficulty you may encounter.
- **Build an Enterprise-wide Plan.** Plan for a recovery that addresses everything from computers to customer service phones to paper-based assets. Every critical function that keeps the business "in business" must be recovered/maintained
- **Exercise Your Plan.** This is a common shortcoming of many well-meaning businesses. The only way you can gauge effectiveness and trouble-shoot weak spots is to test the plan.



Protecting Your Business from the Unexpected

"No matter how well prepared you think you are, there will be some unexpected challenges and expenses."

- **Put Your People First.** Don't lose sight of the human element. Although the survival of the business is at stake, your employees may be facing their own personal tragedies. Include programs to help employees in your business recovery plan (medical care, financial assistance, stress relief, etc.) Unless their families and personal property are safe, your employees will not be focused on recovering the business.
- **Management Must Lead the Process.** Business continuity most often fails when senior management is not fully committed. Not only should the "big guns" be out in front during the planning process, they should also be highly visible during the recovery.
- **Update Personnel on Daily Progress.** Every single employee with a role in the recovery should be updated on its progress. Rumors and misinformation are bad for business and can hamper the recovery process.
- **Build a National Vendor Network.** Some disasters cause damage that is widespread. If it brought you down, it may also have knocked out your local vendors as well. You'd better have a back up supply-line that is out of the line of fire. This includes business continuity vendors, banks and other key suppliers.
- **Anticipate Communications Problems.** Natural disruptions such as earthquakes and hurricanes can bring down phone and power lines. If you don't have access to cellular phones and two-way radios, you might not be able to communicate with key personnel.
- **Expect the Unexpected.** No matter how well prepared you think you are, there will be some unexpected challenges and expenses. Food, for example, is a commonly overlooked expense employees will face while at a distant recovery facility. The company must expect to pick up the tab during most of the recovery process.
- **Use Crisis Management To Your Advantage.** A proactive approach is called for—especially where your customers are concerned. They won't blame you for experiencing a disaster, but they will probably not accept excuses when it comes to the speed of your recovery or the level of your customer service. A little proactive effort on your part can yield handsome returns in customer confidence.



Protecting Your Business from the Unexpected

Who Can Help?

Knowledgeable consultants can help you through this process with an orderly, well-documented methodology. An assessment helps to identify where you have unnecessary exposure to risks and makes cost/benefit-based recommendations. Avoiding problems before they happen may be the best benefit of the Disaster Recovery Assessment.

A good approach is to develop a written report that lists your priorities and the hardware, software, data, and processes that support those priorities. Based on the assessment, our report lays out logical contingency and recovery action plans.

Finally, a written recovery plan provides continuity through staff changes. It can be used to help qualify for recognized quality programs, and potentially meeting insurance requirements.

About the Sponsor

Techcare, through a particular focus in continuing care, ensures our customers gain the maximum value from their IT investments through a progressive set of IT outsourcing services.

Techcare assumes accountability for the management of a variety of Information Technology services including server management, security and availability of the infrastructure, end user support and help desk, hardware repair, and responsibility for helping link technology investments to your business plan.

For more information on how Techcare can deliver the results expected from IT, please contact us at info@techcare.com or by calling 847.374.1600.

