



Microsoft®

SCORE®
Counselors to America's Small Business

Disaster Recovery Planning

How Planning for a Disaster Can Save Your Business

Executive Summary

Target Audience:

Small business owners who are interested in learning about disaster planning best practices to help increase revenue and reduce risks. Special attention is paid to how technology can significantly reduce data loss risks while also benefiting your business.

What You Will Learn:

We will explore the top five reasons your business should have a disaster recovery plan in addition to reviewing disaster recovery best practices to help you start increasing revenues and reducing your business's risks today.

The five best reasons to invest in disaster recovery (DR) planning are:

- 1) Understanding the *real* costs of losing data
- 2) Preventing risk of business failure
- 3) Reducing the risk of liabilities and penalties associated with regulatory compliance
- 4) Increasing employee productivity
- 5) Buying you and your business peace of mind

Tools Included:

This paper provides specific "how to" advice for each best practice cited so that you can immediately implement the ideas you find most compelling. In addition, you are provided websites and other resources for those seeking more information.

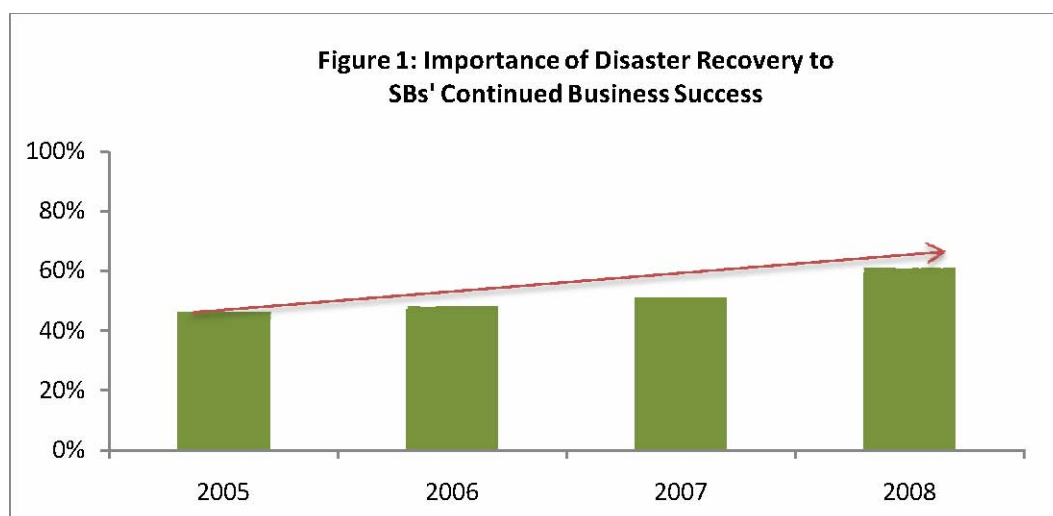
Disaster Recovery Planning

How Planning for a Disaster Can Save Your Business

Do you remember the last time your business experienced data loss and the inconvenience that ensued due to a server crash, lost notebook or simple employee error? Protecting your business data is always important, but during the current economic downturn the stakes are even higher. Small businesses are already feeling the pressure of significant revenue declines, disappearing profits and tightening cash flow. Losing business records or simply being “down” without access to vital customer and invoicing information can make a very challenging economic climate impossible to manage through. The losses in terms of dollar value and time can accumulate quickly as most small businesses today create, acquire and manage more data than ever before via email, spreadsheet/word-processing, accounting and payroll software. If customer data is also involved, the small business will have to confront other unforeseen costs related to legal ramifications of losing sensitive customer data.

Disasters do not wait for a convenient time. Disasters that lead to data loss happen at any time and create just the right situation for your data to disappear within the blink of an eye. Disasters leading to data loss can be caused by natural disasters (earthquakes, hurricanes and floods), technical issues (hard drive failure, virus) or humans (deliberate or otherwise). In fact, 70% of small businesses in the U.S. experienced a data loss in the past year due to technical or human disaster alone [AMI U.S. Small Business 2009 Annual Overview]. Despite these high incidences, few small businesses have a disaster recovery plan to minimize these risks. Interestingly, the absence of a disaster recovery plan isn't due to lack of interest, knowledge or awareness. For example, Figure 1 shows that the proportion has been growing yearly of small businesses.

AMI U.S. Small Business 2009 Annual Overview Study



Many small businesses find the tasks of developing a disaster recovery plan too overwhelming, too expensive or simply something that can be put off until they finally have the time. This paper will provide the guidance you need to implement a disaster recovery plan by helping to remove those barriers.

The purpose of this paper is to help you move from being a small business that is merely interested in disaster recovery to the growing group that realizes they can ill afford to take on any more risks during the downturn and are taking action to ensure their business and its data are properly protected. We will also highlight how a proper disaster recovery plan can benefit your business in other ways including improving employee productivity and potentially increasing revenue.

The first part of this whitepaper explains the risks associated with lackadaisical back-up or disaster planning practices, anecdotes by other small businesses that have “been there, done that” and why they took the leap to develop a back-up/disaster recovery plan. The second portion of this whitepaper lays out specific steps and best practices to help you get your disaster plan up to speed and reduce your business risks.

Part I: Why Your Business Needs Disaster Planning

Disaster planning describes a set of actions to take before, during and after a disaster and should be documented and tested to ensure continuity of operations following a disaster. There are five key reasons your business should be actively pursuing disaster planning today, these five reasons are:

Reason #1: Costs of Losing Data

According to AMI’s 2009 U.S. Small Business Annual Overview Study, 70% of small businesses in the U.S. experienced a data loss in the past year due to technical or human disasters, resulting in an average loss of \$4700 to each small business or \$20 billion industry-wide. Incidentally, these figures do not yet take into account natural disasters (earthquake, hurricane) or opportunity costs of being in business if the data loss did not happen. In this economic downturn, as business dealings are reduced and smaller in value, each customer and transaction is more valuable and can be the difference between being in the black or being in the red each month. It is more important than ever to be able to please and retain your customers, or risk their shopping elsewhere. “Every time we go down I lose at least \$2,000 a day [in business]. Who knows how much it would be if I added it all up, including the amount of time it takes me and my employees to go back to business as usual afterward. It’s painful to say the least,” said Roy Thompson, owner of S&S Body Shop in Northern California.

One small business owner of an online marketing and advertising firm puts his potential losses even higher. “The type of work we do all resides on a hard drive and if that hard drive fails it can add-up to \$40,000 - \$50,000 in lost revenue very quickly,” said Travis Godbout, owner of Propellant. The actual costs vary but the fact that there are real costs related to data loss does not.

Reason #2: Risk of Business Failure

It may sound overstated, but businesses can and have failed when the data they lost is irrevocable. A frequently quoted study by the University of Texas [“Financial and Functional Impacts of Computer Outages of Businesses” 1987] revealed that 43% of businesses that experience a disaster but have no business recovery plan in place never reopen. This is especially likely during the recession, when competitors are aggressively targeting one another’s customer bases and each dollar of revenue comes as result of a great effort. “I’ve never thought of disaster recovery as a competitive advantage but it is,” exclaimed Heather Jacobs of AMS Loans, a small mortgage broker firm. “If our [loan data] was lost tomorrow, we would be fine because we have our data backed-up offsite. However, most of our competitors are just the opposite of us and would have a hard time getting back to business.”

Even if a small business survives the costs incurred from losing data there is no guarantee they will survive the stigma to the business’s reputation, which can be far longer lasting and not easily resolved. Once customer trust has been lost it’s nearly impossible to get it back, or entails significant time and/or money to regain it. Contrast this to the dollars required to plan ahead for disaster recovery and avoid a potential loss, and you’ll see they are merely a fraction of these costs.

Reason #3: Risk of Liabilities and Penalties Associated with Regulatory Compliance

Data continue to grow in importance and relevance to small businesses. Having a robust disaster recovery plan in place today is critical for “offensive” and “defensive” sales purposes and more importantly, in compliance with mandatory business regulations. Having a well thought through set of disaster recovery policies and procedures readily available for clients, customers, vendors and partners to review can be the difference between winning your next project and losing it. As one small business owner described it, “We get most of our business from insurance companies. They are very clear about how long we need to keep records and how their customers’ data can and cannot be used. If we didn’t meet these requirements we wouldn’t have their business. It’s just that clear.”

Non-compliance could result in monetary fines, removal of business license and even prison time. Figure 2 illustrates examples of data retention compliance requirements for all types of businesses and others that are applicable to certain industries.

Figure 2: Example of Data Retention Regulations & Impact of Non-Compliance

Industry	Summary of Regulation	Non Compliance Penalty
Healthcare	To be HIPAA-compliant and to “protect the integrity, availability and confidentiality of medical information,” businesses must retain health records (electronic, written and oral) for a minimum of 6 years.	Fines (up to \$250,000) & possible imprisonment (up to 10 years).
Financial Services including Real Estate	Retained mortgage loan files must be stored for the life of loan and an additional 6-10 years.	Fines (up to \$100,000 for each violation) & possible imprisonment (up to 5 years).

Real Estate	Laws vary by state as well. For example, under California’s Business And Professions Code Section 10148 regulation, real estate companies must retain all listings, deposit slips, checks and other transaction documents for up to 3 years.	Fines & possible suspension or revocation of broker’s license
Financial Services	Under SEC Rule 17a, retain all communication for up to 6 years. It also defines the types of records (e.g. emails), how long and what types of media they must be stored on (e.g. non-rewritable media).	Fines & possible imprisonment
All industries	Following the Fair Labor Standards Act, business must retain employee records related to wages, hours, conditions for 3 years.	Fines (up to \$10,000). Repeat convictions may result in imprisonment.

In addition, having a disaster plan in place could become more important for businesses that participate in government projects. Under the Federal Law Continuity of Services (clause 52.237) or the Office of Management and Budget (OMB), government RFPs may require vendors and their subcontractors to have disaster plans in place, ensure high availability and provide services continually.

There are many publicly documented incidences of firms being fined \$100,000 to \$5 million, \$8 million and even \$10 million due to non-compliance and inability to provide adequate archived data and information on requests. Depending on your line of business, your partners’ and vendors’ requirements will most likely grow on the data management front as will the level of scrutiny from regulators. In fact, they will likely become more stringent with smaller businesses as monitoring technology continues to evolve and improve, making it easier to assess and test for compliance.

There are many resources on the web to help you and your business assess what standards and/or regulations pertain to your line-of-business. Check out www.drj.com for their Disaster Recovery Rules and Regulations information. There you will find a spreadsheet with guidance pertaining to everything from business continuity standards to risk management regulations.

Reason #4: Increased Employee Productivity

Although many businesses employ a disaster recovery plan as a result of a disaster, many other businesses implement these policies and procedures for the productivity gains. Having your data more centrally stored, managed, backed-up and shared can radically improve your firm’s ability and speed to conduct business. Many of the activities related to finding and accessing data are fraught with time-intensive processes and ad-hoc steps that can be greatly minimized if not entirely eliminated. In fact, during a recent AMI U.S. study, when small businesses were asked to select the most important benefit sought from IT investments in the next year, close to a fourth (or 22% of small businesses) responded “improve data management.” As you automate more processes within your business and rely more on technology, data and information management become a more manageable task.

Reason #5: Peace of Mind

Before you downplay the value of this think about how nice it would be to remove data loss from your growing list of worries. For many small businesses it's one of those issues always lurking in the back of their minds, consuming bits of time and thought that could and should be spent on running the business. "When I think of disaster recovery and data loss in general, I think 'nightmare,'" said Janelle McCrackin, a retailer owner. "I've had little data losses here and there with a notebook going down but if I lost it all it would just kill me," said McCrackin. Peace of mind is a real and tangible value that shouldn't be overlooked. It can free-up cycles to focus on more important and productive issues in your business.

Part II: Steps Toward Disaster Planning

We have discussed more than a few compelling reasons why your business deserves and needs to take steps to ensure it has disaster planning and recovery in place. Some of these reasons have to do with risk management while some of them are related to productivity and possible revenue gains. The critical question is how to overcome the myths of disaster planning – how complex, expensive, intimidating or laborious it is – and get started. Below are some easy ways to progress on this front and think about the different aspects of disaster planning.

1. Put your back-up and disaster recovery needs into perspective by "valuing" your data.

Disaster planning and back-up needs may seem even more overwhelming to small businesses if the concept of "data" conjures up images of the business continuously running out of hard-disk space, rapid growth in email volumes or the headaches of safeguarding sensitive customer data. Start off by grouping types of data based on its importance to your business, deciding what you must back-up and recover in the event of a disaster and what you can do without. For data you must back-up, think about what it would cost your business if you lost that data. Try to assign a revenue number to that data in terms of what your business stands to lose (e.g. revenue + time and labor costs). Let this value help justify a specific budget line item for back-up solutions so that you don't find yourself revisiting the question of whether you should be allocating dollars to adequately protect your data.

2. Leverage resources & speak to an IT channel expert or VAR (value-added reseller) that can recommend a data back-up and business continuity solution.

If you are one of the two thirds of small businesses that do not have a full-time IT specialist in your company, consider leveraging the knowledge of a VAR. VARs are IT experts who specialize in adding value on top of IT hardware and software. VARs tend to specialize in installing, consulting, integrating, customizing and/or training users of IT. Often, small businesses can get all of their IT needs fulfilled from one VAR, making their IT experience simpler and more convenient. A discussion with a VAR can clarify your disaster planning needs and solution options. Often times these VARs can help you narrow down your options in a shorter timeframe than going about it on your own. As your business needs change in this economic environment, now is a great time to ask your VAR to recommend storage, back-up and disaster planning solutions that are scalable and allow you to build on them as conditions improve.

3. Communicate your data back-up & disaster planning policies.

Does this sound familiar to your business? “How could you have lost everything? Why didn’t you backup your local files on the server/external hard disk?”

Client back-up (especially notebooks) is often overlooked yet houses essential data. Notebook ownership has risen rapidly in the past few years as prices declined and mobility needs increased. According to AMI’s 2009 U.S. Annual Overview Study, 45% of small businesses currently have a mobile workforce (travels for business at least four to five days per month). Furthermore, eight in ten small businesses use notebooks and makeup a quarter of all PCs small businesses own. However, among notebook-using businesses, slightly more than half of them perform back-up of their data. It is important to communicate to your employees, the importance of data back-up and the company policies of backing up client devices. Implement clear policies and procedures that will become second-nature to your employees to ensure you minimize your risks. Make sure these specific policies are well known throughout your firm and adhered to by everyone.

4. Think beyond onsite back-up.

“I honestly just don’t worry about disaster recovery,” said Melinda Partin, owner of a branding and advertising firm. “Years ago we just asked what would happen if for whatever reason we couldn’t access this building. How would we operate? Those questions quickly took us to solutions like co-locations and daily data back-ups. Now I don’t have to worry about it. ”

Unfortunately, that does not describe a typical small business. Most small businesses that do back-up their data, back-up on site only. This leaves the onsite back-up still vulnerable to theft, human error and natural disasters. Natural disasters are often underestimated in terms of the frequency and damage they can incur. FEMA made more than 550 disaster declarations in the past 10 years throughout the U.S., and these do not include your local fire, flood or electricity outage.

Small businesses should think beyond onsite back-ups and explore offsite options as well. 10% of small businesses currently use storage-as-a-service, a service accessed over the internet where a company (sometimes through a VAR) rents out space on their storage infrastructure to smaller companies or individuals. The service is often priced on a monthly pay-as-you-go basis. Certain storage-as-a-service offerings start around \$10 per month and scale according to the space you require.

When evaluating these storage-as-a-services, focus on the following: how much time and workload it frees up, the lesser likelihood of human error during the back-up process, as well as the ease of how quickly your business can get back up and running following a disaster.

Conclusion: Take Action and Reap the Rewards

Now that you are clearly informed of the risks that face your business regarding data loss and the specific actions you can take to minimize these risks, take action! Be one of the small but growing small businesses that take disaster recovery seriously and use it to make your business stronger and better protected than its competitors.

The time it can take to recover from a massive data loss can range from hours to literally years—if ever. It all depends on what type of solutions and disaster recovery policies and procedures a small business like yours has in place before it happens.

The point to remember in regard to disaster recovery is that there is a major cost associated with doing nothing. Take action now and reap the benefits of having more streamlined and centralized data. The below checklist can be used to help you get started with your disaster recovery planning.

Task Description	Owner	Deadline
Assess the value of your data		
1. Group and classify the different types of data your company uses (between 3-6 types)		
2. Place a dollar value next to each data type based on what it would cost your company if that data was lost tomorrow		
3. Use the different data types (and their associated dollar values) to inform budgeting for data back-up solutions		
Leverage an expert		
1. Contact a VAR and/or IT professional who specializes in data back-up and disaster recovery.		
2. Meet with the expert to discuss your data needs and review the best solutions available to meet your budget requirements (be sure to share the outcomes of step #1 above)		
Develop and communicate clear policies and procedures		
1. Develop a clear and easy to follow set of policies that all employees, partners, vendors and clients can adhere to regarding data use		
2. Develop specific procedures that all employees will adhere to regarding the use of the company's data		
3. Communicate these well defined and easy to follow policies and procedures to your clients, vendors, partners, etc. to ensure they know how seriously you take the protection and proper use of data		

For more information regarding disaster recovery planning please visit one of the below websites:

www.drj.com: Disaster Recovery Journal with tips, tools and other helpful information to ensure your company is up to date on the latest developments and advancements of disaster recovery planning with a focus on best practices and changing laws and regulations.

www.ready.gov/business: A robust government-sponsored site developed in conjunction with the SBA, U.S. Chamber of Commerce and many other agencies. The site includes tips on disaster recovery planning from basic how-to-advice to broader emergency planning guidance.

Since disaster planning and recovery doesn't end with technology, visit one of the below websites to help you plan and be prepared across other aspects of your business needs.

www.stargazer.org: Stargazer provides practical services that actually help people take action to Get Organized, Take Control, Be Informed and Stay in Touch in time of emergency or disaster. The "learn and do" approach of Stargazer enables users to apply simple technology to protect essential information, to alert others about an emergency situation, and to track people and materials.

www.score.org: Includes "how to" articles and tools in addition to helping you find a local small business mentor, at no cost, to help you on a one-on-one basis.

(c)2009 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.