Enterprise Strategy Group | Getting to the bigger truth.™

Market Report

Small Business Data Protection Basics:

What Small Business Owners Need to Know to Ensure Business Continuity

By Lauren Whitehouse

November 2009

© 2009, Enterprise Strategy Group, Inc. All Rights Reserved.

Contents

Introduction 3
Managing and Minimizing Business Risk 3
Business Interruptions 3
Today’s Digital Dependency 4
Protecting Data Protects Your Business 4
The Bigger Truth 4

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of the Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at (508) 482-0188.

© 2009, Enterprise Strategy Group, Inc. All Rights Reserved.

Introduction

When it comes to disasters occurring, the question is not an “if,” but “when.” Disasters can range from an accidental deletion to a small power outage that knocks out communications and computer systems to a weather-related event that wreaks havoc on a region’s infrastructure. What these and other examples have in common is that they all represent the potential for downtime—the period of time when something is not in operation and is inaccessible. For any of the estimated 30 million small businesses in the United States, hours to days of downtime could result in irreparable damage to the company and its reputation. Most small companies prepare for the potential loss of physical assets to minimize the disruption to a predictable level; however, corresponding safeguards to protect digital assets may be overlooked—often with detrimental results.

Managing and Minimizing Business Risk

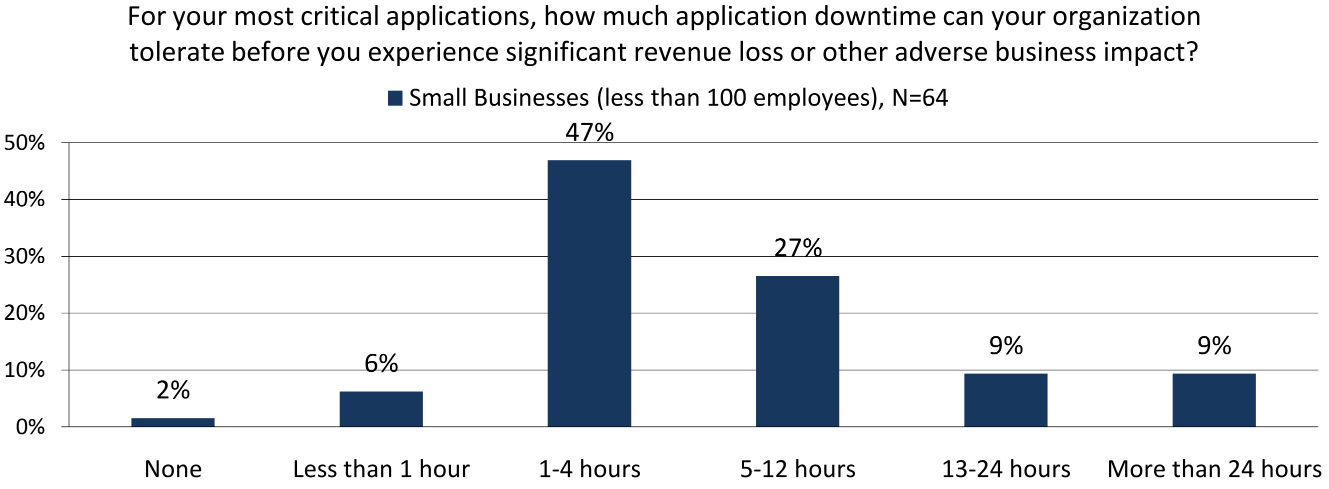
Small business owners and executives typically have contingency plans and insurance policies in place to deal with unforeseen events that affect their businesses. To minimize the risk associated with unexpected events, liabilities, and losses, small businesses take out insurance policies for their assets and develop contingency plans should resources critical to operations not be available. Determining the risk versus investment costs of these protection strategies is straightforward—it boils down to the math. What is the cost of lost revenue versus the premiums or costs incurred to minimize the risk?

The consequences of long-term adverse affects to business due to any prolonged shutdown include lost revenue, customers, employees, suppliers, or partners; damage to the company’s reputation; and even legal liability. Businesses have to be responsive and resilient for any eventuality—seamlessly taking advantage of opportunities while minimizing threats.

Business Interruptions

The threat associated with catastrophic events, such as fires, floods, natural disasters, weather-related events, power outages, chemical or biological hazards, or even acts of terrorism are very real for most companies. Research on the disaster preparedness of small and medium-sized business (SMB) found that 76% of SMBs report that they live in a region that is susceptible to natural disasters.[1] But it’s often the more frequent, mundane nuisances such as malicious tampering, accidents, errors, computer failure, burglary, computer viruses, or hacking events that cause small businesses grief. Research respondents cited three outages within the past 12 months, with the leading causes being virus or hacker attacks, power outages, or natural disasters.[2]

Figure 1. Downtime Tolerance



For your most critical applications, how much application downtime can your organization tolerate before you experience significant revenue loss or other adverse business impact?

Source: Enterprise Strategy Group, 2008.

[1] Source: *Symantec SMB Disaster Preparedness Survey*, September 2009.
[2] Source: *Symantec SMB Disaster Preparedness Survey*, September 2009.

© 2009, Enterprise Strategy Group, Inc. All Rights Reserved.

Interruptions to operations, clearly, could be detrimental to small businesses. ESG research found that 55% of small businesses (those with less than 100 employees) could withstand four hours or less of downtime before suffering adverse business affects (see Figure 1).[3] Of businesses affected by a disaster, *25% never get back up and running*.[4] Being equipped to handle the high-frequency/low-severity incidents that aren't catastrophic, but that happen more frequently, makes small businesses better prepared for larger-scale events.

Today's Digital Dependency

Most small businesses rely on computer systems to keep their day-to-day business running smoothly. Everything from financial records, employee information, customer data and sales orders to video surveillance, e-mail, supply chain data, and third-party logistics information such as shipping and tracking are maintained in digital form. Survey data found that more than half (55%) of SMBs feel they would lose 40% of their company data if their computing systems were wiped out in a fire.[5] As more and more aspects of the business are digitized and automated via the use of computers, the more imperative it is to protect those assets.

Protecting Data Protects Your Business

Small business owners need to proactively protect the computer systems and data needed to maintain business continuity. To ensure a sound data protection strategy:

- **Seek expert counsel.** Just as small business executives might consult advisors for other aspects of their business (accountants, lawyers, etc.), many see the value to leveraging a trusted source—an IT professional, an outsourcer, or a technology reseller or vendor. Communicating objectives and budget guidance is a priority.
- **Determine downtime and data loss tolerance for critical systems.** Two metrics commonly used to evaluate disaster recovery solutions are Recovery Time Objective (RTO), which measures the time between a system outage and the time when the system is again operational, and Recovery Point Objective (RPO), which measures the time between the latest backup and the system outage, representing the nearest historical point in time to which a system can recover. Balancing the desired RTO and RPO with the required capital investment and operational expenses will be key.
- **Protect systems and data.** Based on the required recovery objectives, implement protection strategies such as system-level backup and data backup with copies maintained at a remote location in case the primary location becomes unavailable. Steps taken to ensure the most rapid recovery, such as backing up to disk media and backing up the operating system, applications, configuration settings, and data, will minimize downtime. Performing more frequent backups minimizes data loss. The technology and methods selected should run automatically to free small business executives to focus on running the business.
- **Once implemented, test drive recovery.** Ensure that system and data recovery processes and components meet the required objectives by simulating an interruption and performing a recovery. Make adjustments as needed and revisit drills—at least annually—to ensure preparedness.

The Bigger Truth

Albert Einstein's remark, "Intellectuals solve problems; geniuses prevent them" is fitting when it comes to minimizing risk with respect to loss of access to digital assets. It's a "given" that a small business will experience one or more interruptions of business due to the impact of natural or man-made threats. Small businesses should be proactive in addressing the risk to their business data by putting the right safeguards in place now rather than having to react to an incident after data is compromised. Take the next steps and consult your trusted expert to see what failsafe measures you need to take to protect your data—and your business.

[3] Source: ESG Research Report: *Data Protection Market Trends*, January 2008.
[4] Source: Institute for Business and Home Safety, www.ibhs.org.
[5] Source: *Symantec SMB Disaster Preparedness Survey*, September 2009.

© 2009, Enterprise Strategy Group, Inc. All Rights Reserved.

ESG Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel:508.482.0188 Fax: 508.482.0218 | www.enterprisestrategygroup.com