



Data Backup for Small and Medium Businesses: Priorities, Current Practices, and Risks

November 12, 2008

How safe is small business data?

As the power of computers continues to grow, more and more of the value generated by businesses resides in electronic storage -- everything from customer lists to product plans to accounts receivable. Large enterprises invest heavily in protecting that data by backing it up, using a variety of products and technologies.

But how well protected is the data of small and medium-sized companies? How do those businesses back up their information, and are they doing enough to protect the company against loss? Are their data protection practices keeping pace with the growth of their data?

To answer those questions, Rubicon surveyed computing decision-makers at several hundred small and mid-sized businesses (SMBs) in the United States.

Overall finding: Companies worry about losing data, but their backup practices may not be keeping up.

The survey showed a high level of concern about potential data loss. **Companies rated backup as their #2 computing priority**, after defense against viruses and other malware, and ahead of issues like reducing costs and deploying new computers (page 8). Although most companies do some form of backup, the backup practices they have chosen leave holes in their coverage. Many SMBs rely on manual backup practices that can be forgotten, or even subverted if an employee is disgruntled. And most companies store their backup files in the same location as the computer that was backed up, making them vulnerable to loss through natural disasters or theft.

This whitepaper gives details on the findings from the survey. It's organized into two sections: Impact of data loss on small businesses, and computer backup practices. Here are some key highlights, followed by a more detailed discussion:

- Half of SMBs have lost important business data from their computers.
- A third of the companies that lost data suffered lost sales as a result.
- Although hardware failure is the most common cause of data loss, midsize companies lose data in many different ways, some of them surprising. For example, a quarter of the midsize companies that lost data said they have had incidents in which an employee erased it maliciously.
- About a quarter of SMBs do not back up their servers or PCs.
- Most SMBs are vulnerable to some forms of data loss from their PCs and servers because they store backup files in the same location as the computers backed up.

Half of SMBs have lost data. About half of SMBs have lost data from their computers. In many cases, they were able to recover the lost data from backups, but about 70% of them have lost some data permanently. Page 9.

Impact of data loss: A third have lost sales. Among companies that have lost data, about a third say they lost sales as a result, and 20% have lost customers. Page 13.

As a company gets larger, its risk increases. The rate of data loss is higher in SMBs with over 20 employees. A third of them report losing data several times a year. Page 10.

Causes of data loss are diverse and nonintuitive.

Midsized companies also lose data in more diverse ways than very small ones, and the causes are not necessarily what people would expect. Although natural disasters are often cited as a risk, they are one of the less frequent causes of data loss among midsized companies. Erasure by hackers, deliberate sabotage by employees, and theft all cause more data loss incidents than disaster among midsized companies.

Cause of loss	Suffered by
Hardware failure	63%
Accidental erasure	50%
Software bug	35%
Malware destroyed	35%
Computer stolen	27%
Employee erased on purpose	27%
Hacker erased	25%
Lost password	19%
Fire or other disaster	13%

Leading causes of data loss in companies with 100-250 employees.

This has a couple of important implications. The first is that backup practices appropriate for very small companies may no longer be sufficient as that company grows. The second is that companies -- especially midsized ones -- need to think through all of the different ways they could lose data, and make sure they are protected against all of them. Page 11.

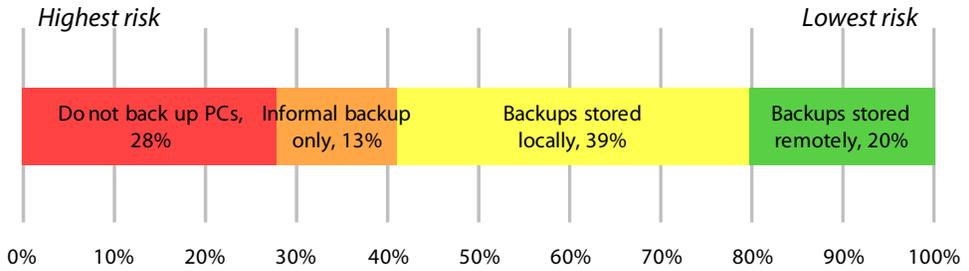
Many companies do not back up their computers fully. About a quarter of SMBs do no backup of their PCs, and another 13% do only informal backup, in which they allow employees to make their own backups, but don't mandate it. Even among companies that proactively back up their PCs, almost two thirds of PC backups are conducted weekly or less often, so data created in the interim is vulnerable to loss. Page 18.

The situation is similar for servers. About a quarter of SMBs with servers do not back them up at all. Among those who do back up their servers, about half are backed up weekly or less often.

Most backup files are not stored remotely. More than half of all backup files are stored in the same location as the originals, which leaves the company vulnerable to permanent loss of its data in the event of hardware theft, malicious destruction of the data, or disaster. Pages 23, 24.

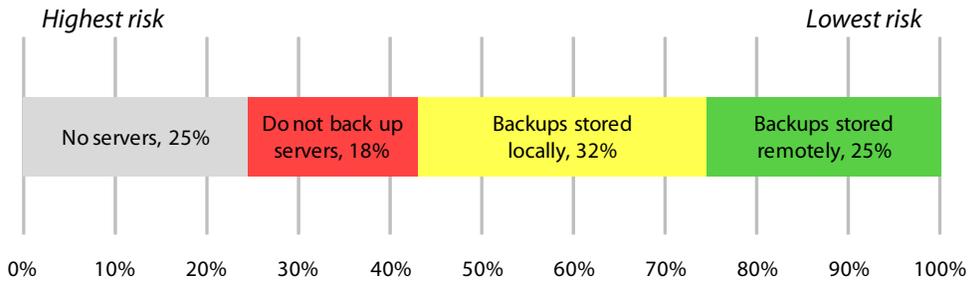
Most companies have somewhat risky backup practices. All backup is not created equal. The charts below summarize the risk level of US SMBs' computer backup policies. In PCs, only 20% of US SMBs are in the lowest-risk category, in which they back up their PCs proactively and store the backups in a remote location. In servers, the rate of remote backup is slightly higher, but still a majority of SMBs do not protect their servers at all, or back up only locally.

PC backup risk



Percent of US SMBs in each category

Server backup risk



Percent of US SMBs in each category

Contents

About this study	6
How to read the charts.....	6
I. Impact of data loss on SMBs	7
Most companies are concerned about the potential for data loss	7
Ensuring data is properly backed up is the #2 priority	8
About half of SMBs have lost important data	9
Frequency of data loss increases as companies grow	10
Hardware failure is the most common cause of data loss, but other causes grow with company size.....	11
Only a quarter of small businesses can always recover lost data	12
About a third of companies losing data have lost sales.....	13
Data loss has severely disrupted a quarter of the companies that lost data.....	14
Cost of data recovery increases with company size	15
Most companies are not completely sure they could recover lost data	16
Speed of data recovery is also critical	17
II. Computer backup practices.....	18
Many PCs are not protected	18
Many servers are not fully protected	19
Many companies don't back up all of their PCs	20
About two thirds of PC backups are not done daily.....	21
About half of server backups are not done daily.....	22
Most PC backups are stored on-site, which creates risks.....	23
Most server backups are stored on-site as well.....	24

About this study

This whitepaper is based on an online survey of US small and medium business computing decision-makers, conducted in September 2008. The survey was designed to explore the overall effects of data loss on small and medium businesses, and to gather detailed information on how they currently back up the information on their PCs and servers.

The survey covered 318 decision-makers in companies with fewer than 250 employees. Results were segmented by company size, and an overall result was also calculated, with weightings based on US Census data. The survey should have a margin of error of about four points at the 90% confidence level.

The respondents were sourced from an independent sampling firm.

Symantec funded the research, but Rubicon conducted the research independently and Symantec had no influence over the results.

How to read the charts

The survey results were segmented by company size (number of employees):

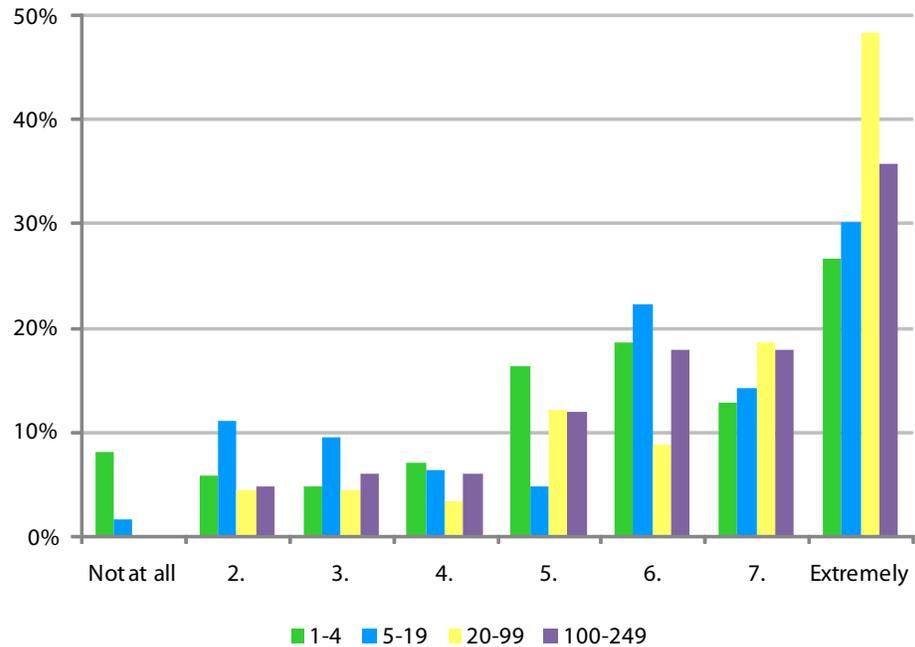
- 1-4 employees (shown in green on the charts, unless marked otherwise)
- 5-19 employees (shown in blue, unless marked otherwise)
- 20-99 employees (shown in yellow, unless marked otherwise)
- 100-249 employees (shown in purple, unless marked otherwise)

In most of the charts, the bars show percent of total respondents in each of the company size bands. Other scales are explained in the notes below the charts.

I. Impact of data loss on SMBs

Most companies are concerned about the potential for data loss

About half of computing decision-makers in the survey said they are very concerned that their company might lose data stored on its computers (7 or 8 on a 1-8 scale). Most of the rest were moderately concerned.



Percent of respondents giving each response

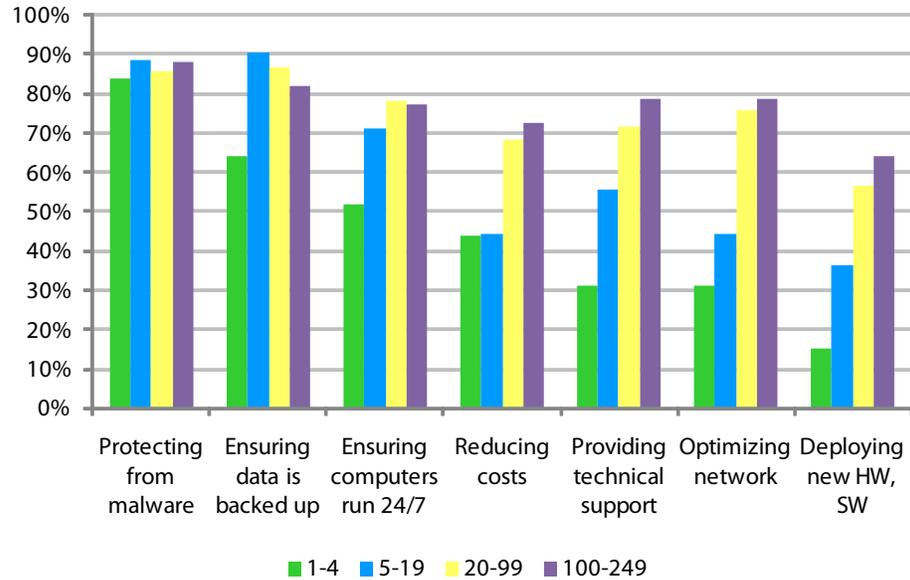
Question: "How concerned are you about the risk of losing important business data stored on your company's computers?"

Base: All respondents

Ensuring data is properly backed up is the #2 priority

The survey gave a list of common business computing priorities, and asked decision-makers to rate the importance of each one. Ensuring that data is properly backed up was the second highest priority, after protecting against malware attacks.

Companies with over 20 employees gave a high rating to a larger number of issues, which is to be expected since they typically have more complicated computing environments.



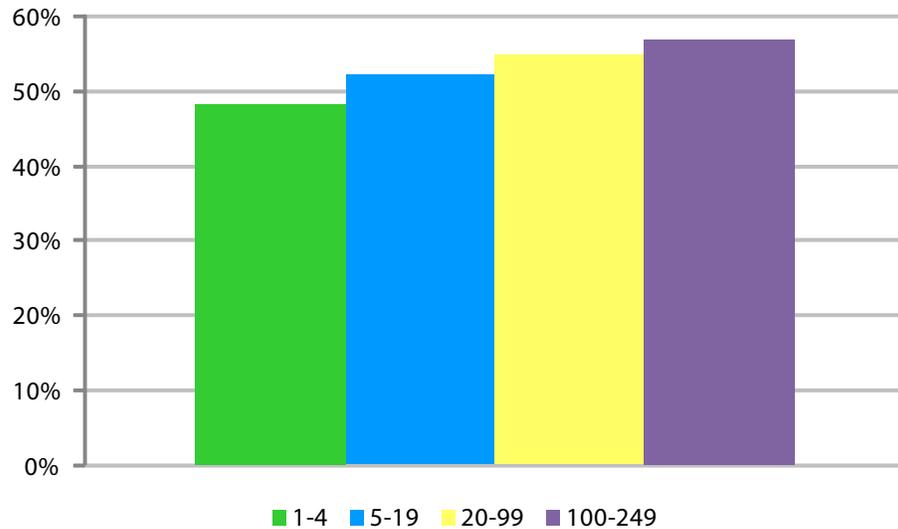
Percent of respondents rating an issue 7 or 8 on an 8-point scale.

Question: "Please rank the following computing priorities in order of their importance to your company (on a 1-8 scale, 8=extremely important)."

Base: All respondents

About half of SMBs have lost important data

Even the smallest companies experience significant rates of data loss, with almost half of companies with 1-4 employees losing data.



Percent of small companies saying they have lost data

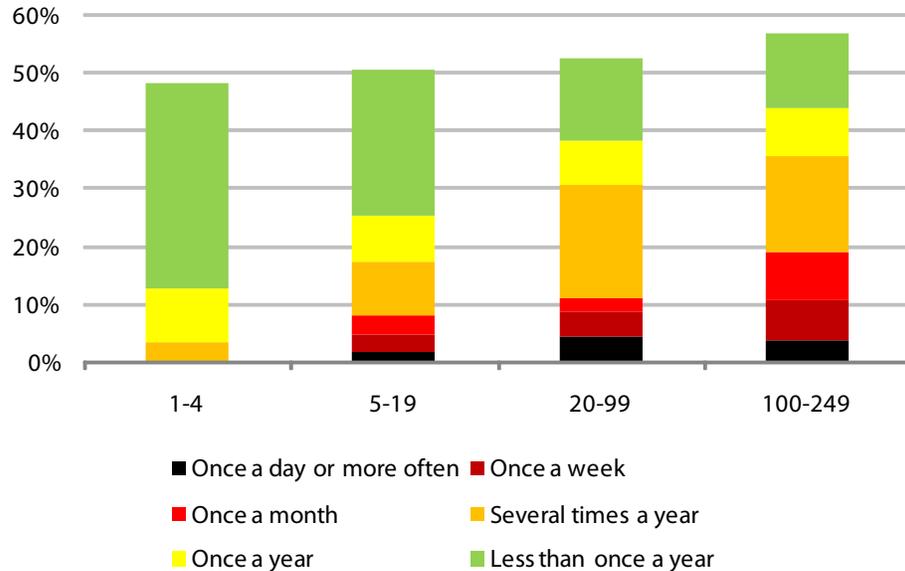
Question: "Has your company ever lost important business data that was stored on one of its computers?"

Base: All respondents

Frequency of data loss increases as companies grow

This chart has the same base as the previous one, but now shows how often companies lose data. The larger a company is, the more frequently it loses data. That's no surprise -- bigger companies have more computers, and therefore more opportunities to lose data.

About a third of small companies with 20 or more employees lose data several times a year.



Percent of all small businesses losing data

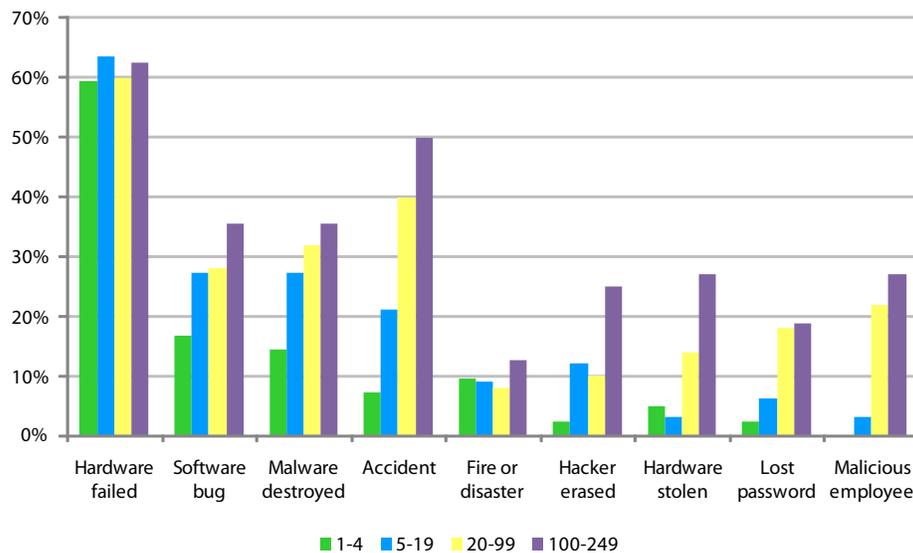
Question: "On average, about how often has your company lost important business data that was stored on a computer?"

Base: All respondents.

Hardware failure is the most common cause of data loss, but other causes grow with company size

Failure of a computer or disk drive was the most common cause of data loss. But other causes were also very prominent, especially in companies over 100 employees. Accidental erasure, malware, software bugs, theft, hackers, and employee sabotage were all important causes of data loss in those companies.

This finding implies that companies should revisit their backup strategies as they grow. Practices that gave good protection to a very small company may be insufficient as that company grows beyond 20 employees.



Percent of companies that have lost data to causes listed. More than one answer allowed.

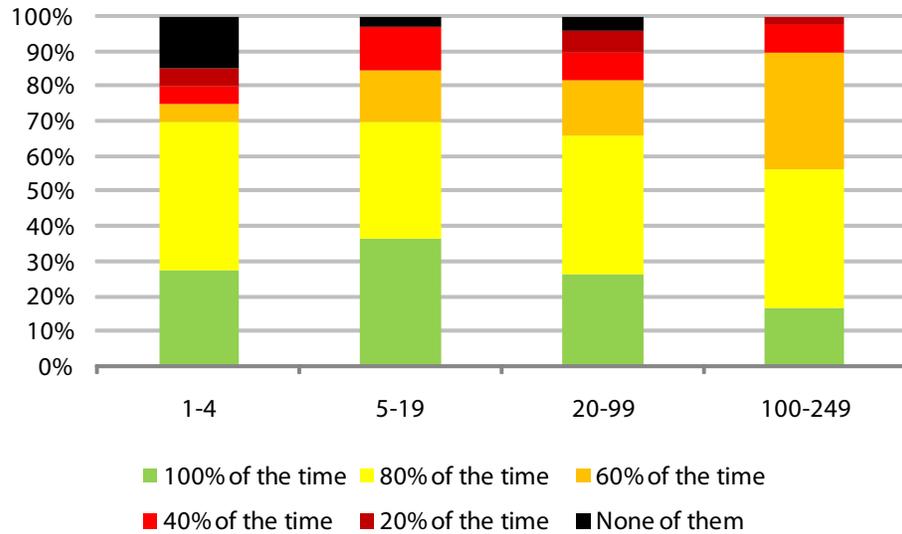
Question: "How did you lose the data in those incident(s)?"

Base: Companies that have lost data.

Only a quarter of small businesses can always recover lost data

Although most companies do some sort of backup today, they can't always recover lost data. In fact, only about a quarter of small businesses reported that they can always recover data they lose.

The smallest companies had the highest rate of permanent data loss, with 15% of companies with 1-4 employees saying they *never* have recovered any lost data.



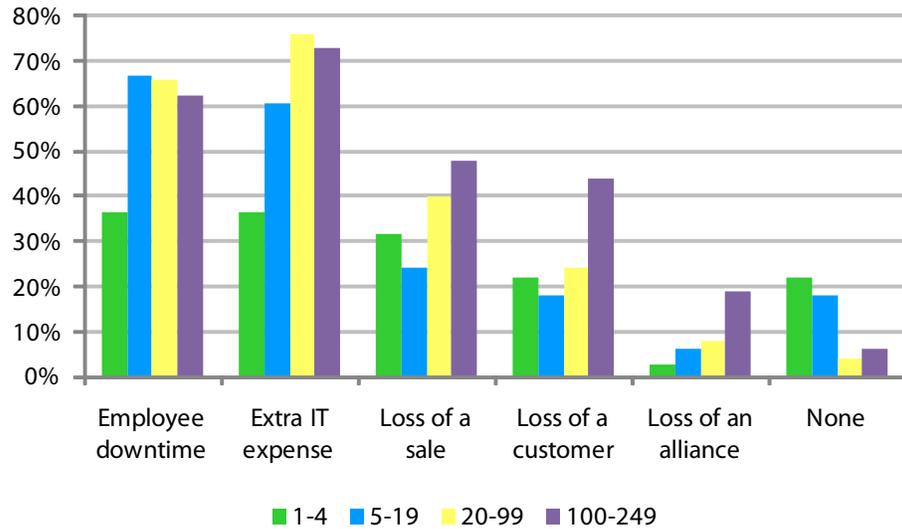
How often data is recovered, by company size.

Question: "In what percent of your data loss incidents have you been able to recover the lost data?"

Base: Companies that have lost data.

About a third of companies losing data have lost sales

About a third of the companies that lost data said they have lost sales or a customer as a result. The impacts were most severe for small companies with more than 100 employees. Almost half of them have lost sales.



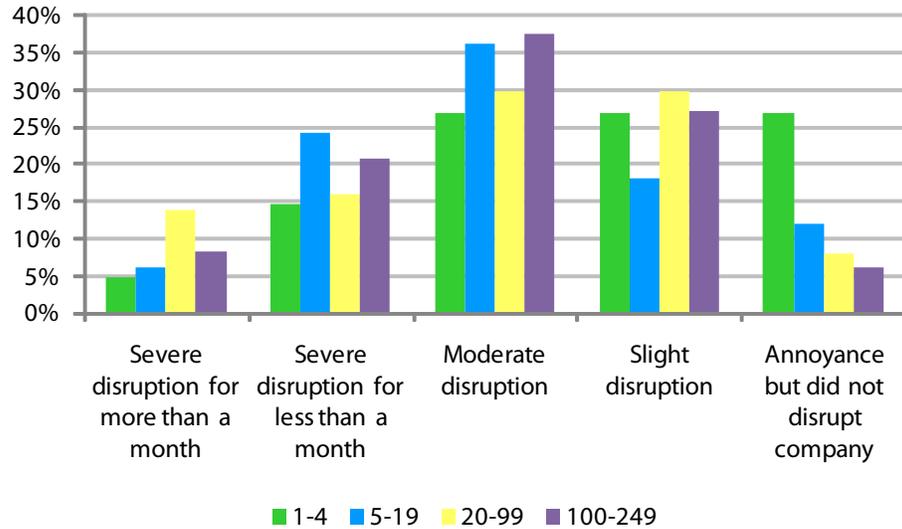
Percent of companies reporting each impact

Question: "Have data losses ever caused any of the following problems at your company?"

Base: Companies that have lost data.

Data loss has severely disrupted a quarter of the companies that lost data

Companies that had lost data were asked about the impact of the loss. About a quarter of them said data loss had caused severe disruptions to the company.



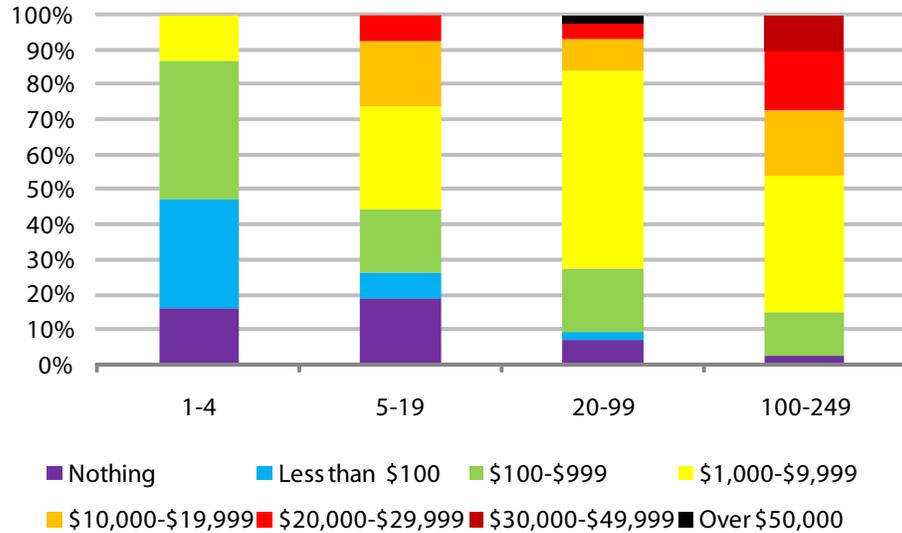
Percent of companies reporting each impact

Question: "Think about the worst incident of data loss that your company has ever had. Please choose the phrase that best describes the impact of that data loss on your company."

Base: Companies that have lost data

Cost of data recovery increases with company size

As a company gets larger, the cost of a data loss incident gets higher. Almost half of SMBs over 100 employees have spent over \$10,000 recovering lost data. Half of companies with 5-19 employees have spent \$1,000 or more.



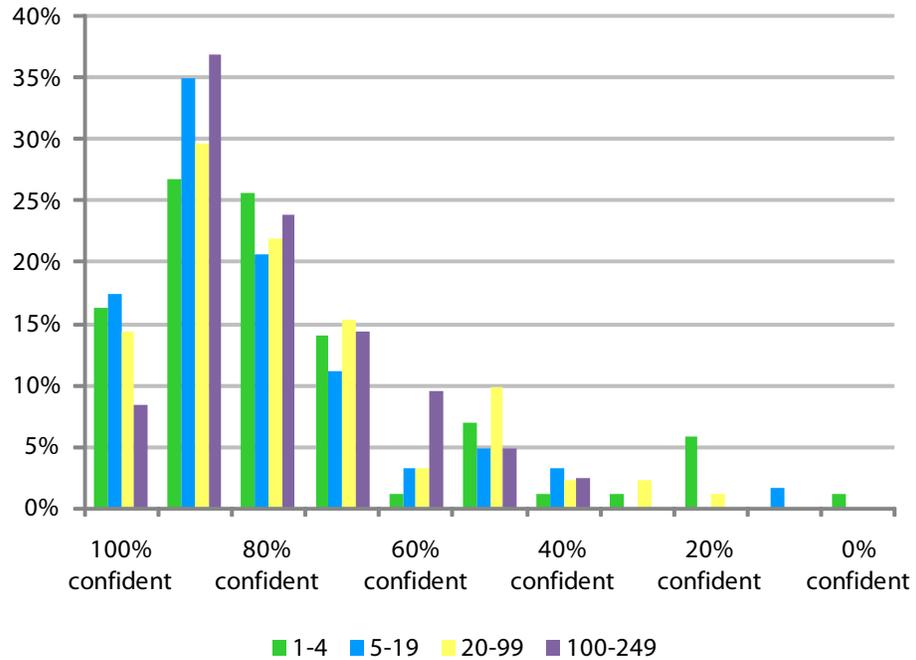
Percent of companies in each size band reporting different levels of data recovery cost

Question: "What is the largest amount of money your company has ever spent to recover lost data?"

Base: Companies that have lost data.

Most companies are not completely sure they could recover lost data

Most companies are fairly confident that they could recover data if they lost it, but very few of them are completely sure. Only about 10-15% of small companies were 100% confident that they would be able to recover data if they lost it.



Percent of companies at each confidence level.

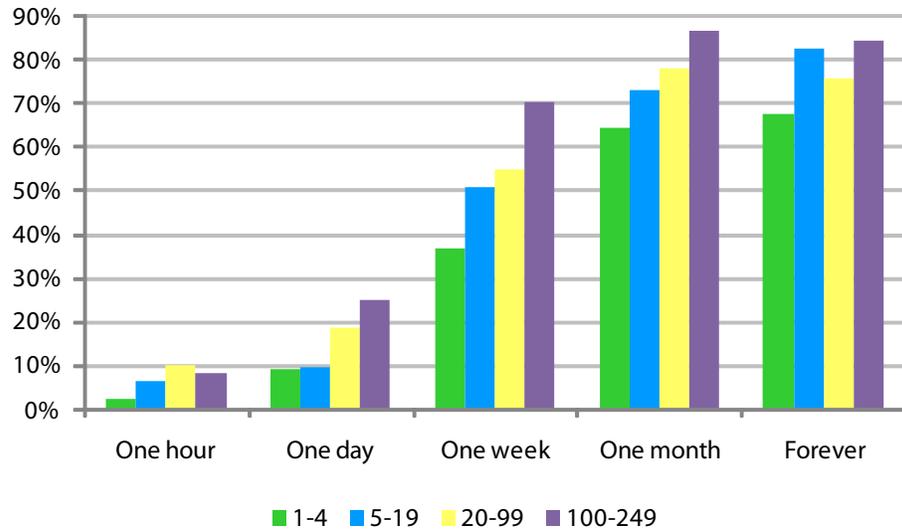
Question: How confident are you that if your company had a data loss, you would be able to recover it?

Base: All respondents.

Speed of data recovery is also critical

Even if a company's data is backed up, the company also needs to consider how quickly it can recover the data. This question asked about the impact of losing access to all of a company's data for varying periods of time.

Even a relatively short period of loss would have a strong impact on many firms. For example, about a quarter of midsize businesses (100-249 employees) said they would lose some business permanently if they lost access to their data for a single day.



Percent who responded, "We might permanently lose some business."

Question: "Please choose the phrase that best describes the impact on your company if it were to lose access to all of the information stored on its personal computers and servers for the following periods of time."

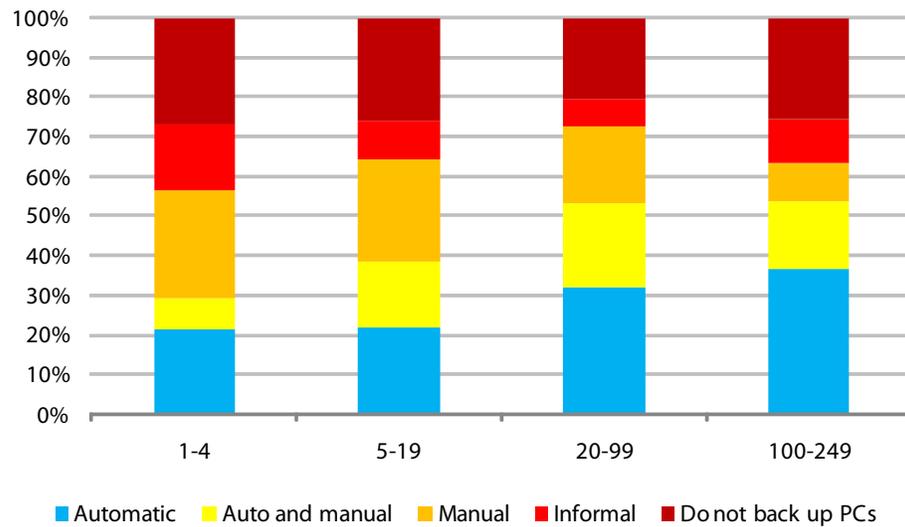
Base: All respondents.

II. Computer backup practices

Many PCs are not protected

About 40% of SMBs do very little to back up their PCs: 28% do nothing to back up their PCs, and another 13% do only informal backup, in which they trust employees to back up on their own but the company does nothing proactive.

Among companies that do perform proactive backups, many use manual backup systems (such as manually copying files to a CD or hard drive). Automatic backup systems, or a mix of automatic and manual, are more likely to be used in businesses over 20 employees.

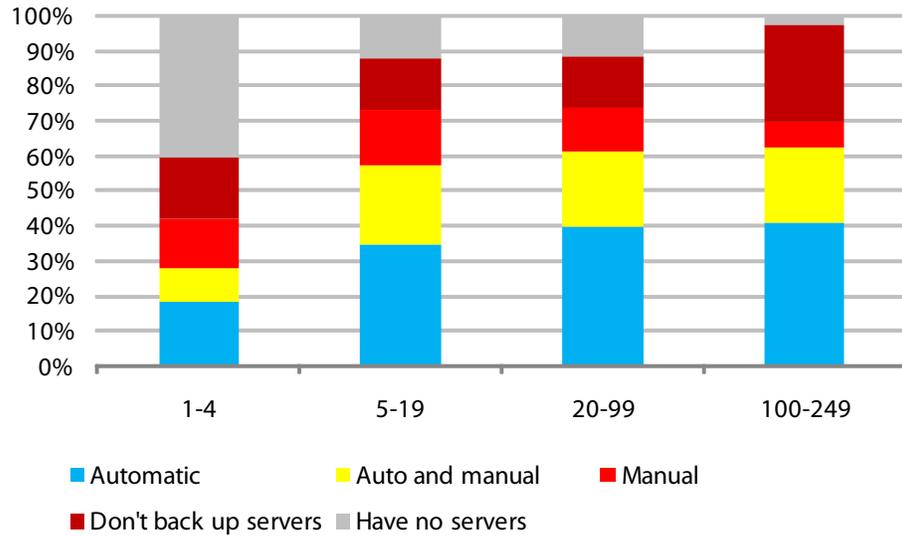


Percent of companies using each PC backup practice.

Base: All respondents.

Many servers are not fully protected

Servers are a little more likely to be backed up than PCs, but still significant numbers of them are unprotected. For example, about 30% of companies over 100 employees do not back up their servers.

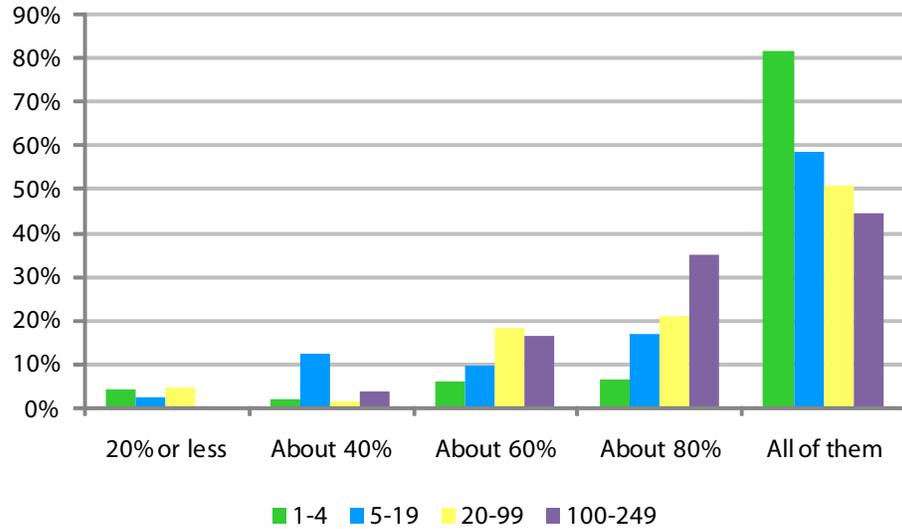


Percent of companies using each server backup practice.

Base: All respondents.

Many companies don't back up all of their PCs

Among the companies that back up their PCs proactively, the smallest businesses are most likely to back up all of their PCs. About half of the companies with over 20 employees do not back up all of their PCs.



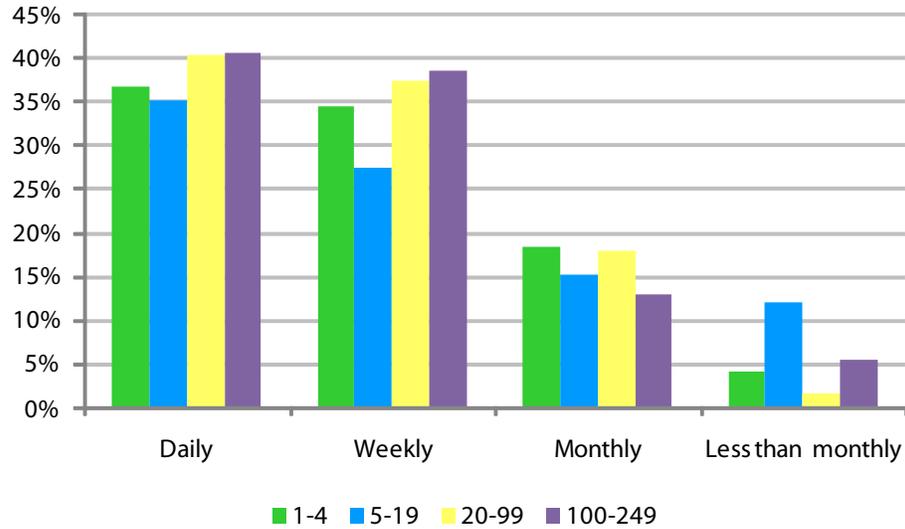
Percent of companies at the various backup levels.

Question: "About what percent of the PCs used by your company do you back up?"

Base: Companies that proactively back up PCs (excludes informal backup and no backup).

About two thirds of PC backups are not done daily

Many PCs are at risk of losing data created since the last backup. About a third of the PCs that get backups are backed up once a day. Another third are backed up once a week, and the remaining third are backed up less frequently.



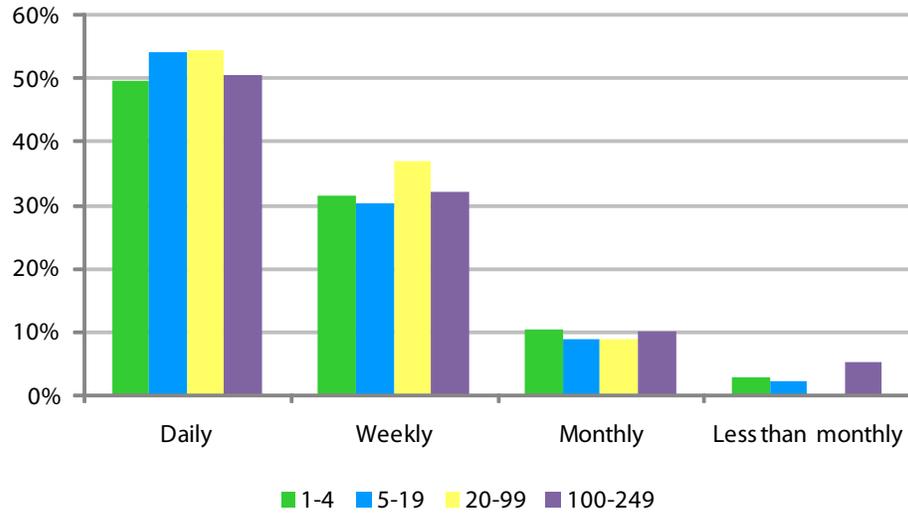
Percent of companies backing up their PCs at each frequency.

Question: "On average, how often do the PCs get backed up?"

Base: All companies that proactively back up PCs.

About half of server backups are not done daily

Recent data is also at risk on many servers. About half of server backups are conducted daily. A third are weekly, and the rest are less often.



Percent of companies backing up their servers at each frequency.

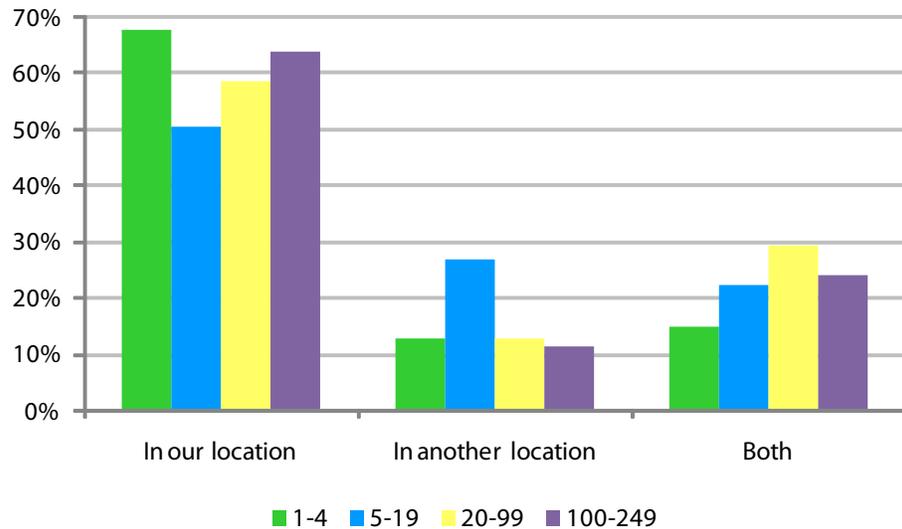
Question: "On average, how often do the servers get backed up?"

Base: All companies that back up their servers.

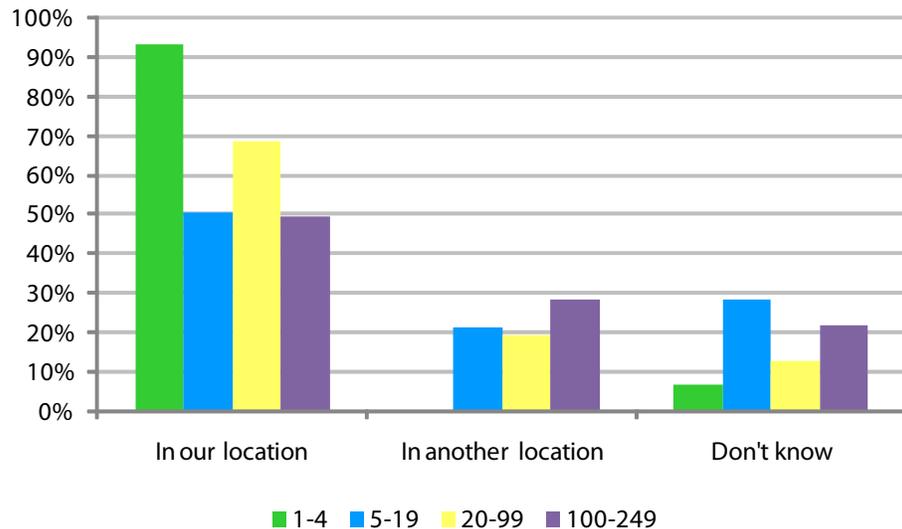
Most PC backups are stored on-site, which creates risks

Most PC backup files, whether they were made automatically or manually, are stored in the same location as the original files. This exposes them to potential loss in a theft, sabotage, or natural disaster.

Where manual backup files of PCs are stored



Where automatic backup files of PCs are stored



Percent of companies using each storage location.

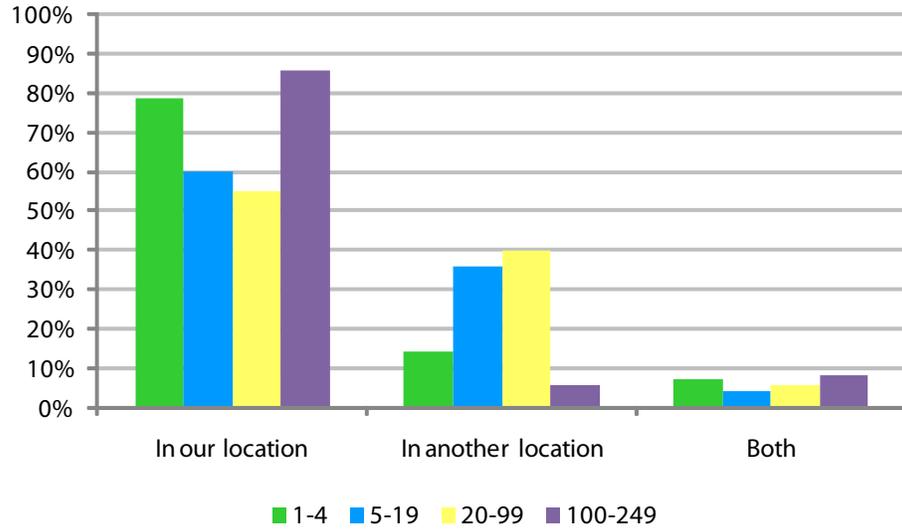
Question: Where do the backups get stored?

Base: Companies that back up PCs.

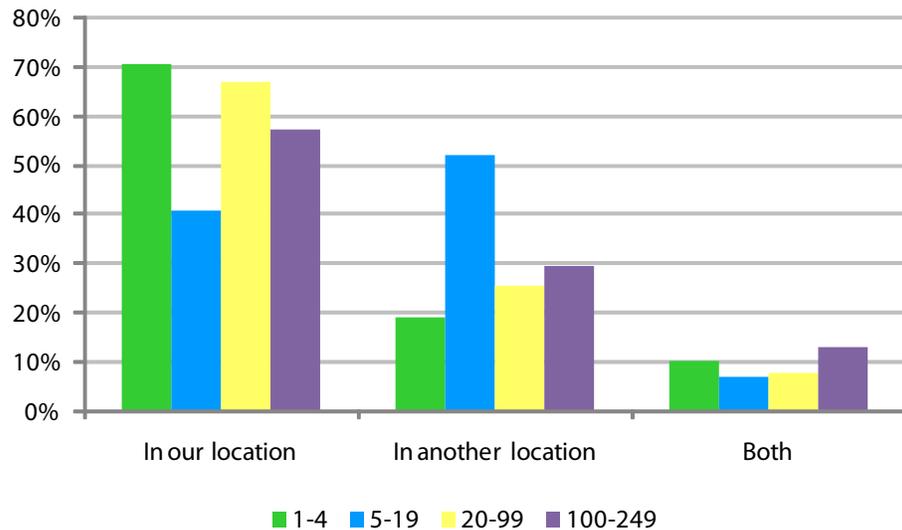
Most server backups are stored on-site as well

As was the case with PCs, more than half of server backups are stored in the same location as the servers.

Where manual backups of servers are stored



Where automatic backups of servers are stored



Percent of companies using each storage location.

Question: Where do the backups get stored?

Base: Companies that back up servers.

About Rubicon Consulting

Rubicon Consulting is a strategy and marketing consultancy designed specifically for the needs of tech companies, from today's global giants to tomorrow's. Rubicon's proprietary methodology delivers significant material results to clients, driving revenue growth, market share, and profits. Rubicon clients include Adobe, Autodesk, Hewlett-Packard, Logitech, Nokia, Openwave, Symantec, Symbian, VMWare, and numerous small web and software startups.

Rubicon's insight has helped its clients thrive through the rise and fall of numerous paradigms, from the PC era to the graphical OS wars, e-commerce, Web 1.0, Web 2.0, and the rise of mobility. The firm combines the intellectual rigor and wisdom expected from a giant consulting firm with the savvy and hands-on focus of veterans from some of Silicon Valley's best companies.

The company's website is: www.rubiconconsulting.com