WHITE PAPER: SMB SURVEY

SMB Protection Gap

SMB security and data protection: survey shows high concern, less action

White Paper: SMB Survey

SMB Protection Gap

SMB security and data protection: survey shows high concern, less action

Contents

Introduction

Small and mid-size businesses (SMBs) are major contributors to business innovation, value, and growth-many expect them to take the lead in global economic recovery. So a 2009 survey showing widespread and serious information security vulnerabilities in this crucial business segment is cause for genuine alarm.

This paper will outline that survey's findings, focusing on areas where even modest investments by SMBs can generate major returns in IT security, data protection, and business confidence.

At a glance

A Symantec survey of SMBs conducted in 2009 revealed that:

- Security and data protection are top SMB priorities
- Despite those priorities, many SMBs fail to act on their legitimate concerns
- Survey participants blame staffing, budget, and time constraints for the gap
- Stable to growing budgets at SMBs suggest that they understand the importance of IT security and are taking practical steps to improve it

About the survey

Applied Research surveyed 1,425 small and mid-size companies across 17 countries for Symantec in February 2009. Results covered the full spectrum of industries, regions, and company sizes:

Geography		Size (employees)	
North America	28%	10 – 100	44%
Latin America	21%	101 – 250	28%
Europe	9%	251 – 500	30%
Asia/Pacific/Japan	42%		

Survey details and additional findings are available here. The survey questions corresponding to the data in the Figures are listed in the Appendix.

Priorities and concerns

In February, 2009, participants in a global survey of small and mid-sized businesses (see "About the survey" on the following page), reported information-security concerns and goals as shown in Figure 1.

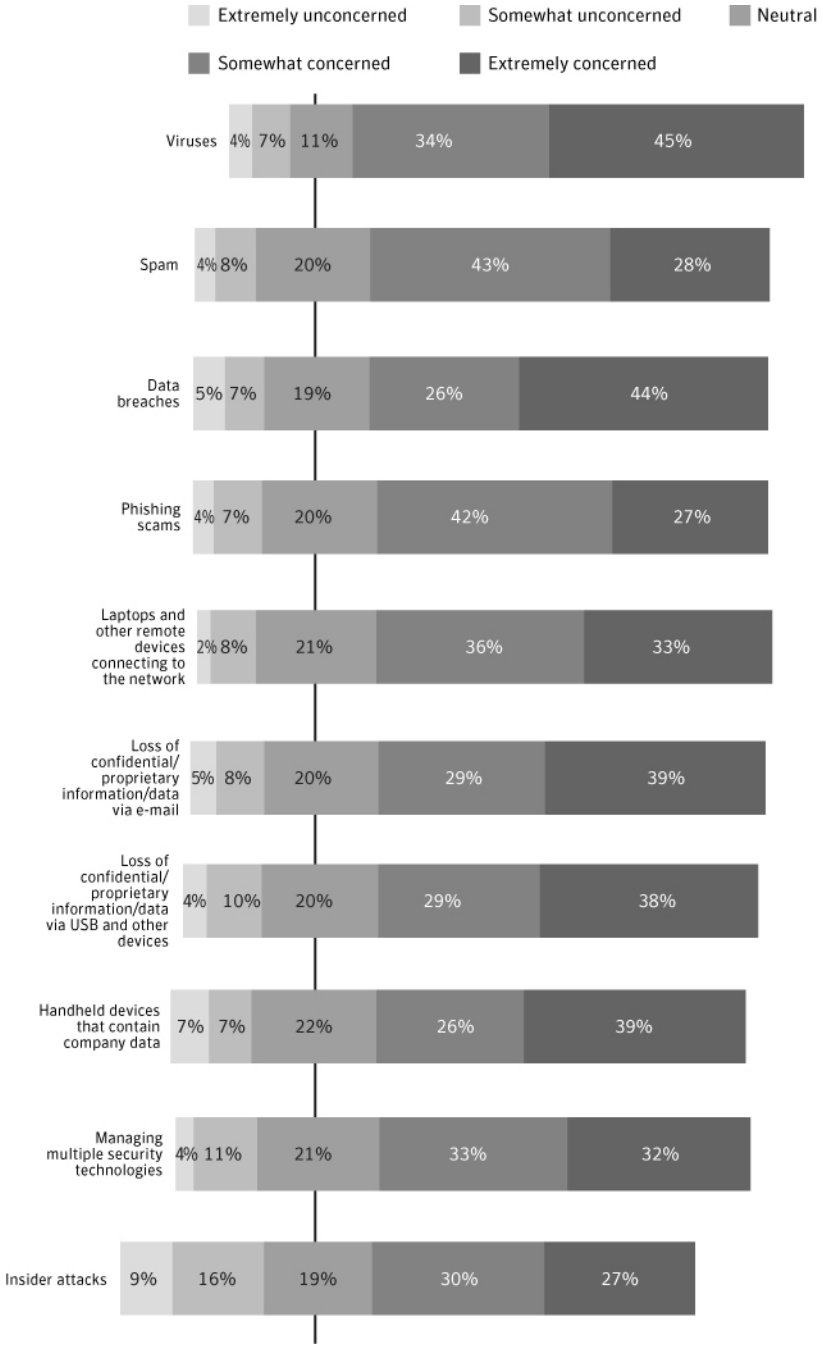

Figure 1: SMB risk-awareness and security priorities

Self-ratings of security concerns and priorities by 1,425 small and mid-size businesses. The vertical line indicates the center of the "neutral" response category. Note the low rates of "extremely unconcerned" and "somewhat unconcerned" categories

(in dark blue), and high "somewhat concerned" and "extremely concerned" ratings (in light blue) for such key security issues as virus defenses, information protection, and backup/recovery.

These results show a high level of general concern about security issues: there is no single issue about which a majority of participants feel unconcerned, or even neutral. What's more, their priorities are clear: viruses are one of their top security issues, with 79% of participants reporting themselves extremely or somewhat concerned-followed by spam at 71% and data breaches at 70%. Among their security goals, protecting information takes priority over networks and servers.

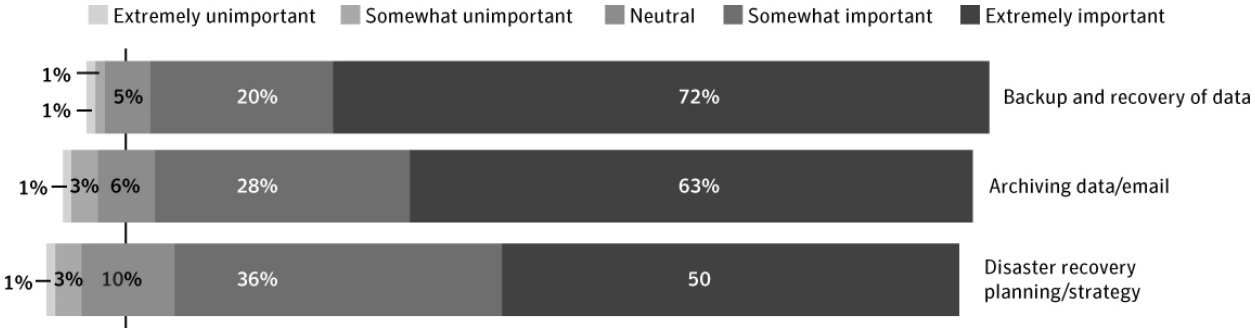

Figure 2: SMB data-protection priorities

SMB self-ratings of data-protection concerns and priorities. The vertical line indicates the center of the "neutral" response category. Note that a large majority of participants rated all data-protection issues as important, with backup and recovery showing a slight lead.

SMBs view data-protection issues as important even more consistently than they do security issues. Figure 2 shows that backup and recovery are their top data-protection priority, with a slight precedence over disaster recovery and archiving.

In short, small and mid-sized businesses have focused an appropriate level of concern on the business risks that affect them most. The next-and far more important-question is how they will reduce those concerns, address the risks by actually implementing solutions to protect their businesses.

The protection gap

But despite awareness of the risks they face and clarity about the best ways to mitigate them, a striking number of small and mid-sized businesses not only trail the state of the art, but lack even the most basic protection for their business information. Figure 3 shows the status of planning and implementation across the segment.

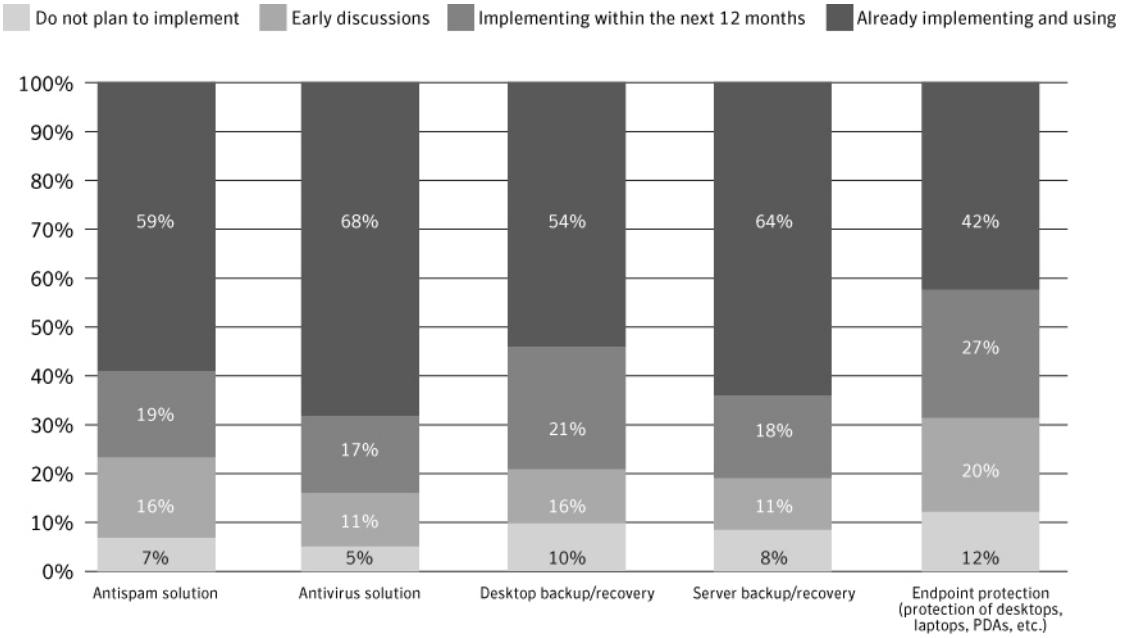

Figure 3: Information defenses in place or planned

Security and data-protection initiatives planned or in place at participating firms. Note vulnerabilities in endpoint protection, desktop and server backup/recovery, and even basic antivirus and antispam coverage.

More than a third of these businesses operate with no protection against viruses and spam. Many others are protected only by half-measures: backup/recovery for servers but not desktops for example, or antivirus point solutions that can't protect mobile endpoints or defend against fast-changing, fast-moving, complex threats that use multiple techniques to attack digital assets. As Ray Boggs, Vice-President of SMB research for IDC puts it, "Of course SMBs know better, but they are too often focused on business opportunities outside the company to pay attention to the risks they are taking right at home."[1]

1-Ray Boggs. In "Small and midsized businesses aware of security risks, but not doing all they can to protect information." Symantec Corporation press release 20090409_01. (Cupertino, CA: Symantec Corporation. April 9, 2009), http://www.symantec.com/about/news/release/article.jsp?prid=20090409_01.

What's stopping them? Through the survey, SMBs report the familiar constraints of staffing, time, and budget, as shown in Figure 4:

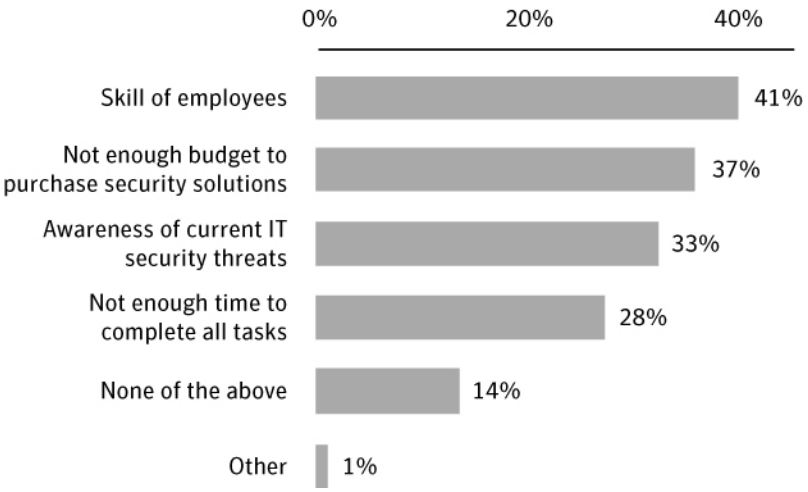

Figure 4: Root causes for the protection gap

Reasons reported for security gaps at participating small and medium-size businesses. Note the predominance of staff, time, and budget constraints.

These limits are especially severe at businesses that lack even a single in-house dedicated IT staff member-true for 42% of survey participants. What's more, their median IT security and storage budgets hover around $4,500 per year-barely enough to keep up with obsolescence, much less growth. The survey did reveal one promising trend-despite downdrafts throughout the economy as a whole, 90% of SMB survey participants reported their IT security and storage budgets trending up, or at least not in decline.

Consequences

To assess the economic scale of the risks these firms face, the survey asked participants who had suffered security breaches or data loss to inventory the conditions responsible. And as Figure 4 details, those conditions strongly resemble the inventory of SMB security risks reported in Figure 1:

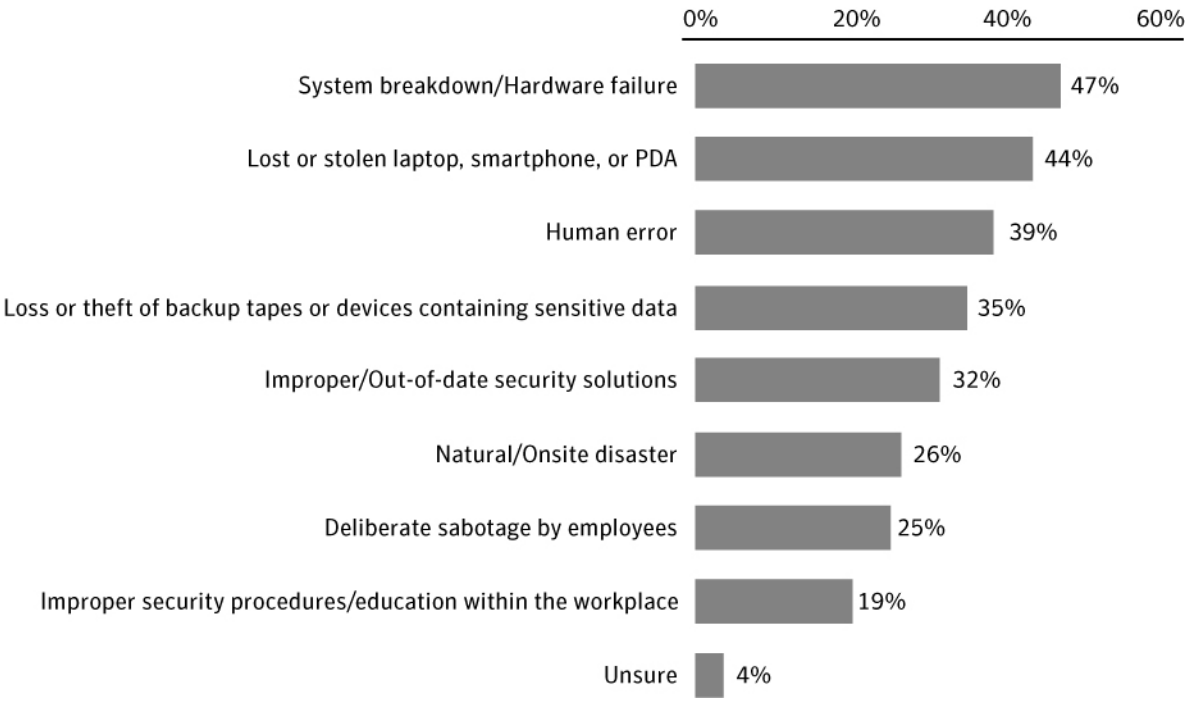

Figure 5: Causes cited for security breach or data loss incidents. Sources of SMB security and data breaches
Reported causes of security and data loss incidents at surveyed companies. See text for correspondence between these causes and vulnerabilities reported in Figure 1.

Not surprisingly, a cross-comparison of Figure 5 against Figure 1 shows that security incidents and data losses are concentrated exactly where SMB gaps and shortfalls leave vulnerabilities. Here are just a few examples:

- 44% of breaches involve compromised mobile devices-endpoints like laptops and PDAs that are overlooked in many SMB security plans
- 39% involve sabotage, human error, or poor procedures-while SMB security concentrates on threats from outside the network
- 35% of breaches involve failures in backup processes-known vulnerabilities for SMB servers, desktops, and laptops

Solid, regular backup practices can mitigate the risks of inevitable hardware failures, but lapses may have serious consequences-a separate study[2] by Rubicon Consulting showed that SMB data loss incidents are followed by lost sales in 30% of cases, lost customers in 20%, and severe business disruption in 25%.

Protection principles

Losses and business risks like these are not necessary. Even when staff, time, and budget constraints stand in the way of a systematic solution, small and mid-size businesses can improve their security posture with simple, cost-effective protection measures like these:

Stay informed

Some of the best things in IT security are free. Information resources won't keep technical defenses up to the minute, but periodic reports like the Symantec Internet Security Threat Report can keep even the smallest business aware of trends in the threat environment, and how best to defend against them.

Back up data

They may be tedious and time-consuming, but backups-even manual backups-offer some of the highest returns available among IT initiatives. Protection against natural disaster, hardware failure, and above all human error gives a business continuity and confidence in the face of a wide range of risks. Include off-site storage of encrypted data as part of a mature backup and recovery program.

Protect from the inside

Employee error, fraud, and vandalism can compromise a company's most sensitive and valuable information-and legally required disclosures can savage its reputation. Simple policies and controls-starting with elimination of duplicate or portable data stores-can substantially improve your security posture. The Payment Card Industry offers excellent guidance on data protection, appropriate for members and nonmembers alike.

Don't forget physical security

By far the oldest component of data protection, physical security still ranks high in importance. Policies for screen-locking, end-of-day shutdown, asset tagging and tracking, and others are easy to implement-often as simple as keeping the right doors locked. And every one of them cuts the odds of the worst-case data-loss scenario, when a device containing critical data falls under a thief's control for an extended time with low chance of exposure.

When the time comes to invest in upgrading your electronic protection, here are three additional principles to consider:

Use layered security

Threats escalate, and even sophisticated protections can fail against new attacks. Multi-layer defenses protect against local breakthroughs or single-point failures of any one technology or method. The latest defense-in-depth strategies combine antivirus and antispam software with firewalls, intrusion prevention, device and application control, and patch management solutions.

Deploy comprehensive security

Depth is critical, but don't neglect breadth. Security plans should cover desktops, laptops, and messaging servers. Mobile devices-whether carried in by outsiders or taken out by employees-are the most difficult to protect. But new endpoint

2-Rubicon Consulting. Data Backup for Small and Medium Businesses: Priorities, Current Practices,

protection technologies quarantine connections until new devices demonstrate compliance with all relevant security policies, and ensure that security products are regularly updated to block new threats.

Use solution providers for needed expertise

You are exposed to a single company's security and threat environments, but your local solution provider sees tens-even hundreds. If staffing and time constraints are keeping you from effective information protection, your local IT consultant or reseller can help you explore a cost-effective way forward.

Consider Symantec

Symantec can help at every stage of your security and data protection development. An abundance of free resources available through the company's website include virus scan and removal tools, information to help you clarify your security priorities, and of course the industry's broadest range of security, infrastructure, and management software.

Symantec's latest security offering, Symantec Protection Suite (SPS), is designed, scaled, and priced to meet SMB security and data protection requirements. The only suite offering comprehensive protection across laptops, servers, messaging gateways, and backup and recovery environments, SPS delivers proven protection for business information and computers, helps defend against aggressive new malware and spam threats, and backs up and quickly recovers computers and information in the event of a problem.

Appendix

Text of survey questions illustrated in Figures:

Figure 1

Text of survey question:

How concerned are you about the following security issues?

a) Viruses

b) Phishing scams

c) Spam

d) Laptops and other remote devices connecting to the network

e) Handheld devices that contain company data

f) Data breaches

g) Managing multiple security technologies

h) Insider attacks

i) Loss of confidential/proprietary information/data via email

j) Loss of confidential/proprietary information/data via USB and other devices

Figure 2

Text of survey question:

Rate the importance of each of the following backup and storage goals:

a) Archiving data

b) Backup and recovery of data

c) Disaster recovery planning/strategy

Figure 3

Text of survey question:

What are your plans for each of the following solutions?

a) E-mail archiving

b) Antispam solution

c) Antivirus solution

d) Backup/recovery

e) Replication

f) Online storage

g) Short-term storage

h) Long-term storage

Figure 4

Text of survey question:

Among the following, which would you say are the top barriers preventing your company from creating a more secure environment? Please select up to two responses.

a) Not enough budget to purchase security solutions

b) Not enough time to complete all tasks

c) Skill of employees

d) Awareness of current IT security threats

e) None of the above

f) Other

Figure 5

Text of survey question:

Why did the security breach happen? Please check all that apply.

a) Improper/out of date security solutions

b) System breakdown/hardware failure

c) Loss or theft of backup tapes or devices containing sensitive data

d) Lost or stolen laptop or smartphone

e) Natural/onsite disaster

f) Deliberate sabotage by employees

g) Human error

h) Improper security procedures/education within the workplace

i) Unsure

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
20330 Stevens Creek Blvd.
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

8/2009 20094842