SMB Threat Awareness Poll

GLOBAL RESULTS
CONTENTS

Introduction .................................................................................................................................................4
Methodology ................................................................................................................................................6
Finding 1: Small businesses have a strong interest in virtualization ................................................. 8
Finding 2: Small businesses are still grappling with how to adopt virtualization...............10
Finding 3: Perhaps due to the immaturity of this market, Small businesses are neglecting to
protect their data and systems in virtual environments .................................................................12
Symantec Recommendations ..................................................................................................................14
SMB Threat Awareness Poll

Global Findings

Executive Summary

Information is the lifeblood of most organizations, and SMBs are managing more of it than ever before. Personal customer information, proprietary product information and employee credentials are among the valuable items cybercriminals have set their sights on. This information has become as valuable to criminals as cash, and they are developing more creative and effective ways to steal it. From attacks kits to phishing to social engineering scams, criminals are setting their sights on SMBs.

A secure, operational network lies at the heart of any successful business. The goal of every SMB is to keep valuable data secure in the face of growing attacks. How well you protect yourself against these attacks can mean the difference between a successful year and the failure of the company itself.

Symantec conducted its SMB Threat Awareness Poll in September 2011, asking 1,900 SMBs how familiar they are with threats, and what they are doing to protect themselves. The results show that organizations are aware of the threats, but they feel that their small size makes them less vulnerable to attack. This, in turn, means SMBs are not doing everything they could to secure their valuable information.
METHODOLOGY

Symantec commissioned Applied Research to conduct the SMB Threat Awareness Poll in September 2011. They contacted 1,900 organizations globally with between 5 and 499 employees. Of those businesses surveyed, 25 percent had 5 to 50 employees, 25 percent had 50 to 99 employees, 25 percent had 100 to 249 employees, and the remaining 25 percent had between 250 and 500. The survey respondents were those responsible for managing the organization’s computing resources.

The poll has a reliability of 95 percent confidence with +/- 2.2 percent margin of error.
FINDING 1

SMBs are familiar with security threats.

First, we wanted to see just how aware businesses are of the security threats that are out there, so we asked about their familiarity with the following:

- Distributed Denial of Service attacks
- Shortened URLs
- The use of mobile devices for business
- Keystroke logging
- Targeted attacks

The research found that businesses are familiar with security threats, with 55 to 59 percent of respondents stating that they were “somewhat” or “completely” aware of each of the dangers.

Organizations also showed good general awareness of how these threats could pose a security risk to the organization. More than half (54 percent) stated that malware would reduce productivity while the infected systems were repaired and 36 percent recognized that hackers could gain access to proprietary information. Forty-six percent noted that it could cause a revenue loss.

They are also aware of the negative impact that targeted attacks could have on the business. Forty-six percent said that a targeted attack would cause a revenue loss and 20 percent said it would drive customers away.

The numbers are encouraging, although there is still clearly room for improvement among SMBs in recognizing how cyberthreats – particularly data theft – can negatively affect the organization.
FINDING 2

SMBs don't think they’re a target for cyberattacks

SMBs know that these threats exist, but they don’t feel they are at risk. With so many well-publicized attacks in recent months on businesses throughout the world, why would these SMBs feel relatively little concern over cyberattacks? Half reported that the reason for their lack of concern is because they are a small business and are therefore not a target for cyberattacks. However, that’s not the case. According to data from Symantec.cloud, since the beginning of 2010, 40 percent of targeted attacks have been directed toward small businesses, compared to only 28 percent that have been directed toward large enterprises – showing that SMBs are gravely underestimating their risk.

Given this lack of concern, then, our next finding should come as no surprise.
FINDING 3

SMBs are not taking action to protect themselves.

SMBs are not doing all they can to keep their information and resources safe from cyber threats, since they don’t consider themselves vulnerable. When it comes to DDoS attacks, for example, 56 percent of businesses believe they are protected – but 61 percent don’t even have a written plan for dealing with them. More than a quarter (28 percent) believe that DDoS attacks only happen to larger companies.

When it comes to safeguarding online banking credentials, nearly two-thirds (63 percent) secure machines used for transactions. On the plus side, two-thirds of them do restrict who has access to login information, but nine percent don’t take any special precautions at all.

Unfortunately, even basic malware safeguards are somewhat lacking among SMBs. Several additional findings highlight further security concerns:

- 67 percent don’t use web-based security/service
- 61 percent don’t use antivirus on all desktops
- 47 percent don’t use security on mail server/services
- 40 percent don’t use a security suite on all desktops

Q101: What do you do for malware protection?

- Nothing, because we don’t have a problem with malware
- Use a full security suite on all desktops
- Use security on mail servers/services
- Use AV on all desktops
- Use web-based security/service
- Restrict who has access to login/password
- Lock down machines used for online banking
- We don’t do online banking

What do you do to protect your company’s online bank account?

- We don’t do online banking
- Restrict who has access to login/password
- Lock down machines used for online banking
- Use a full security suite on all desktops
- Nothing, because we don’t have a problem with malware
- Use security on mail servers/services
- Use AV on all desktops
- Use web-based security/service

Q101: Does your company have a plan in place in the event it becomes the victim of Distributed Denial of Service (DDoS)?

- Yes, we have a written plan
- No plan, and I’m not sure what to do
- We’re a small company and Distributed Denial of Service (DDoS) only happens to large companies
- Yes, but I know what to do
Symantec Recommendations

Just because a business is small doesn’t mean it is invisible or immune to security concerns. Based on the results of the survey, Symantec has developed the following recommendations to help SMBs improve their security posture and keep their networks – and business – running:

- **Educate employees**: Develop Internet security guidelines and educate employees about Internet safety, security and the latest threats. Part of the training should focus on the importance of regularly changing passwords and protecting mobile devices.

- **Assess your security status**: SMBs are facing increased risks to their confidential information so safeguarding data is critical. One data breach could mean financial ruin for an SMB. Know what you need to protect. It’s important to understand your risks and security gaps so that you can take steps to protect your information.

- **Take action**: Be proactive and develop a security plan. Consider items such as password policies, endpoint protection, the security of email and Web assets, and encryption. You should also evaluate whether on-premise or a hosted service would best suit the needs of your organization.