

---

## Security survey in United States

This document contains the results of a survey on network security in 455 small and medium sized businesses, conducted in the United States in October/November 2007.

---

## Contents

Contents .....	2
Introduction.....	3
The survey.....	4
Summary of findings.....	5
The results.....	6
Analysis .....	12

---

## Introduction

This document contains the findings of a survey carried out in the United States that examined the state of, and approach to, security among small and medium sized businesses. The survey was commissioned to eMediaUSA who were responsible for the collection of the data.

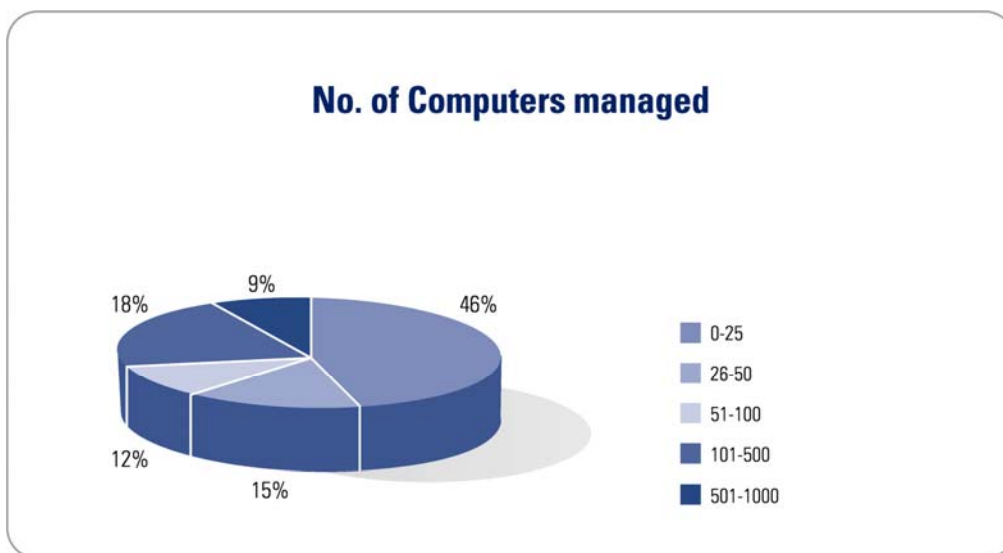
The survey was distributed by eMediaUSA in October and ran for a period of four weeks. A total of 455 companies or institutions in the United States replied. The respondents were senior executives or senior IT administrators and they represent the whole spectrum of companies that fall into the SMB sphere, which is defined by GFI as a company having between 5 and 1000 seats. A full breakdown of the respondents according to company size is provided.

---

## The survey

The 12 questions cover a range of security topics that are of importance and of concern to IT and security administrators in SMBs. The questions were drafted to give a snapshot of the state-of-security in SMBs and to confirm or otherwise issues that have been raised in a strong body of independent security research carried out this year.

A total of 455 respondents completed the questionnaire. The majority of respondents (46%) are companies between 0-25 seats. Forty-five percent are representative of companies having between 26 and 500 seats. The remainder (9%) covers companies with 501+ seats.



---

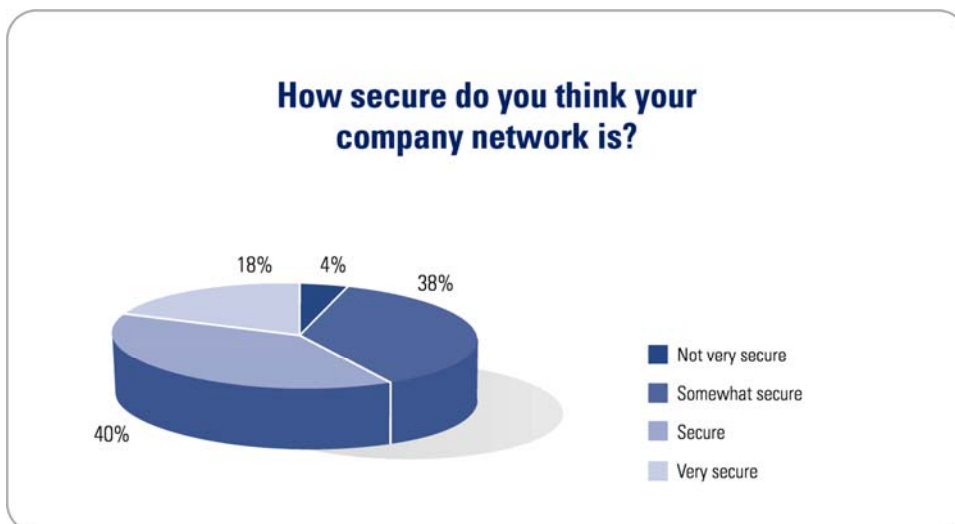
## Summary of findings

The following are the salient findings from the survey:

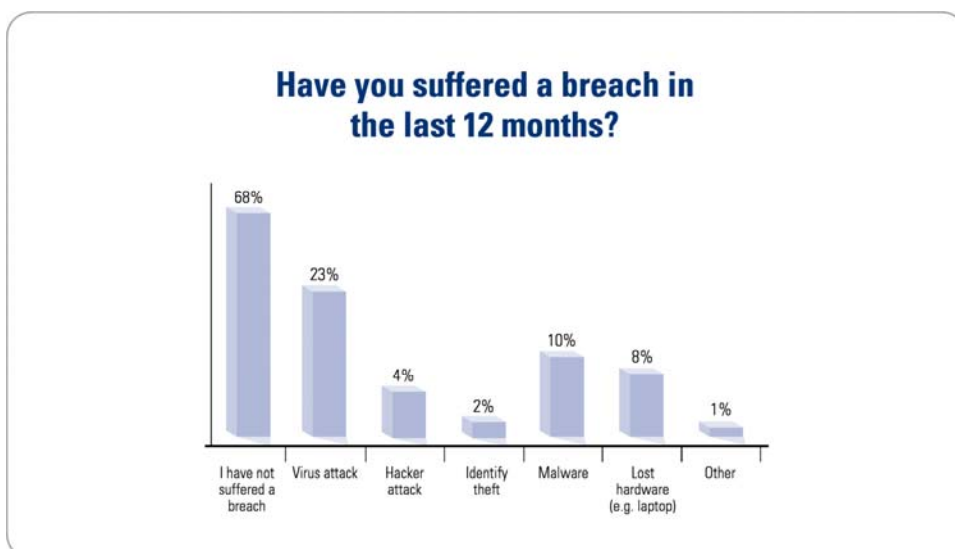
- 42% of US SMBs, or 4 in 10, do not consider their networks to be secure
- 32% of SMBs have suffered a breach over the past 12 months
- 96% and 93% have anti-virus software and firewalls; 80% have anti-spam products
- 55% use a combination of software, appliances and hosted services to protect their network
- 71% say downtime and security issues are their main daily IT concerns, 51% identify user support as a major daily concern
- 39% say email viruses are the greatest security risk
- 55% of SMBs spend 10% or less of their IT budget on security measures
- 77% say this budget is enough to cover their security requirements
- 48% believe that better awareness on security among employees would improve the level of security while 25% want senior management to be more aware of security issues.

## The results

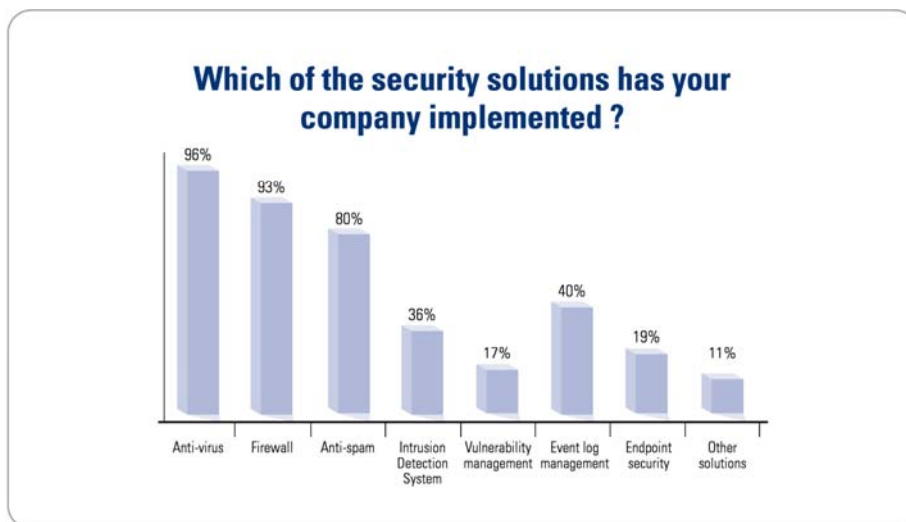
### Question 1



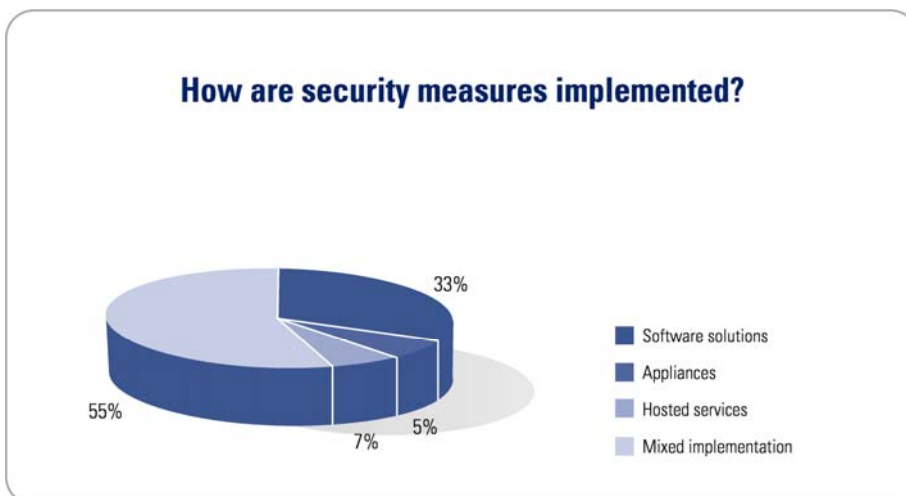
### Question 2



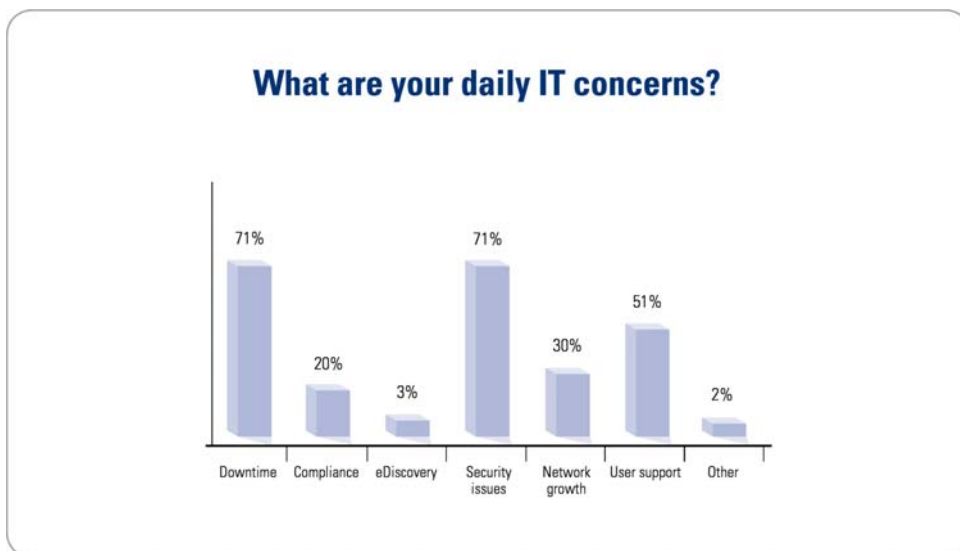
### Question 3



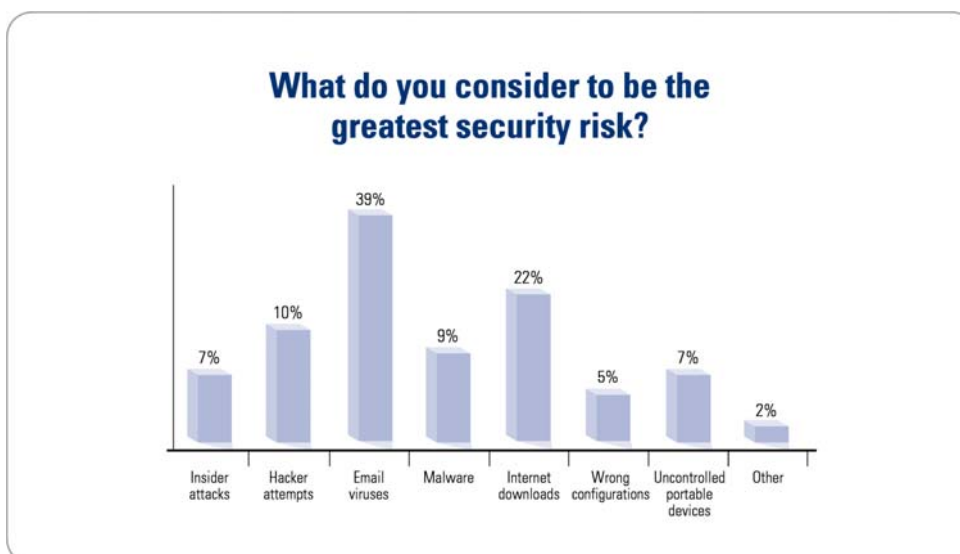
### Question 4



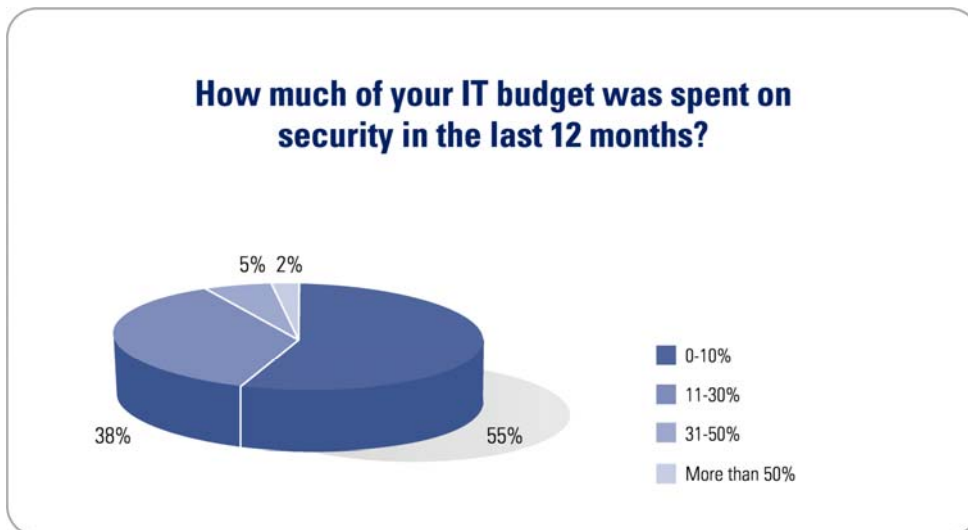
### Question 5



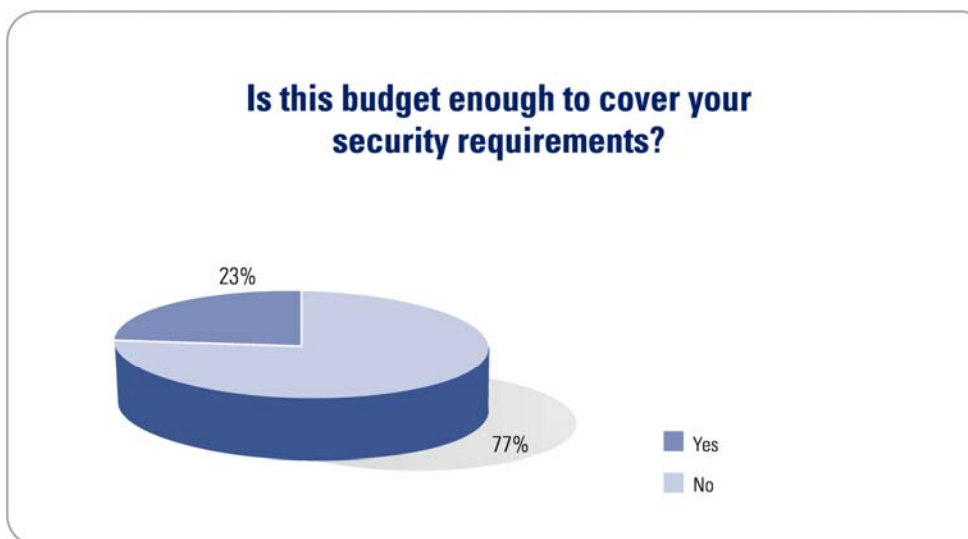
### Question 6



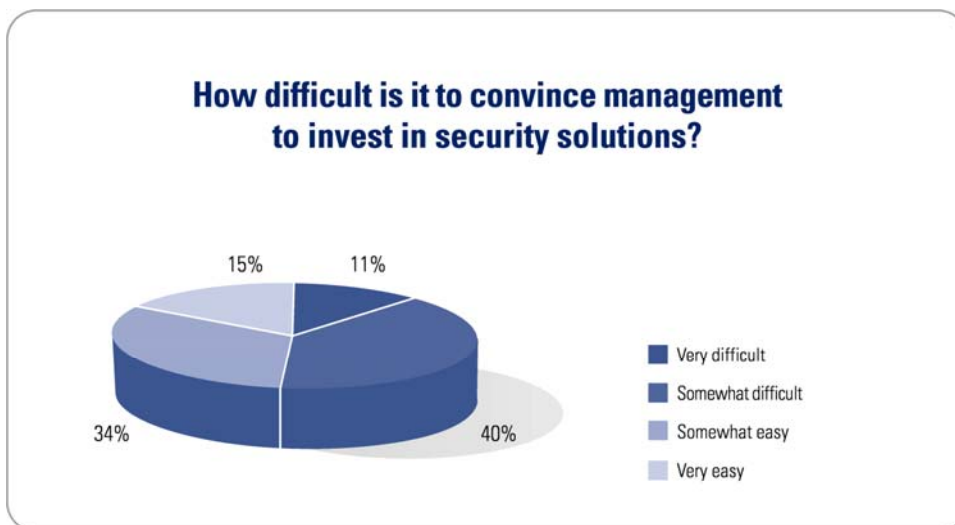
Question 7



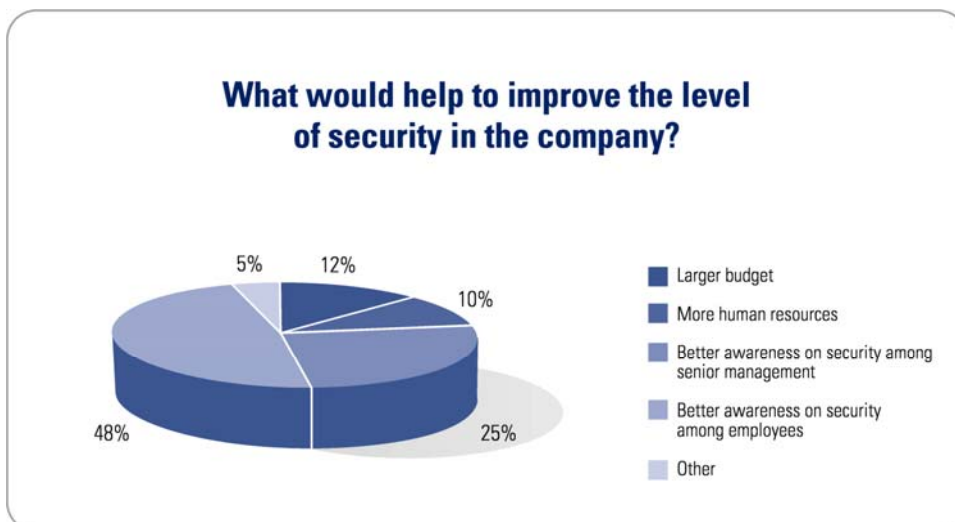
Question 8



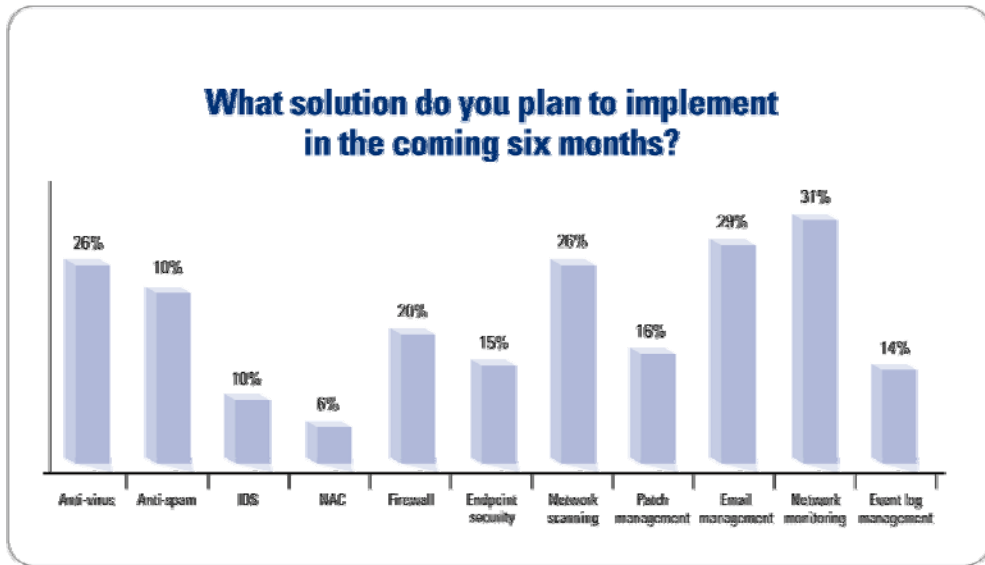
Question 9



Question 10



Question 11



---

## Analysis

The results of the survey cover three areas of interest: network security; education and budgets.

The following is a breakdown of the results according to these areas:

### NETWORK SECURITY:

**Despite having anti-virus and anti-spam software as well as a firewall installed, four in 10 small and medium sized companies in the United States still do not believe their networks are secure.**

42% said their networks were not secure even though 96% and 93% of respondents respectively said they had anti-virus and a firewall installed. 80% said they also used spam filtering. This may indicate that small and medium sized businesses are starting to doubt the effectiveness of traditional perimeter security products in protecting them from other security threats, including data leakage and network breaches.

**39% of respondents said email viruses are the greatest risk to network security, followed by internet downloads (22%) and hacker attempts (10%). Only 7% considered insider attacks and the threat of portable storage devices – such as USB sticks, CDs, floppies, smartphones, MP3 players, handhelds, iPods, digital cameras – to be the greatest risk.**

32% had suffered a breach over the past 12 months; mainly due to a virus attack (69%), followed by infected internet downloads (30%) and loss of hardware, e.g. laptops (24%). Only 2% reported a breach involving some form of fraud or identity threat.

**Email viruses top the ‘greatest threat to network security’ list and this is not surprising. It is one of the easier attack routes and this is confirmed by those respondents who reported a breach. While companies are tackling viruses and malware, they appear to be giving sparse attention to other equally dangerous threats such as data theft and leakage from endpoints such as connected USB sticks, iPods and PDAs on the network.**

Only 19% of the respondents said they had deployed an endpoint security solution on their network. This indicates that few companies may consider the fact that an employee's iPod or USB stick can be a threat and used to copy data from the network or else install unauthorized software or upload viruses and malware.

**On a daily basis, IT executives are most concerned with downtime (71%) while more than half of the respondents said daily user support was a concern. One in five said**

**compliance was a daily concern; while a mere 3% indicated eDiscovery to be a daily issue.**

When it comes to choosing the type of security measure to adopt, just under 90% said they used a software solution with 55% opting for a combination of software, appliances and hosted services.

#### **EDUCATION:**

**Nearly half of small companies in the United States believe that employees with a better knowledge of security issues and the part they play in a company's IT set-up would help to improve network security, a new survey shows, while one in four say that even management should be more aware of security issues and threats.**

48% said that awareness on security issues among employees – the 'weakest link' – was key factor that could lead to better overall security.

**Employees are not the only people who need to be 'educated'. One in four IT executives want senior management to have a better understanding of security issues as this could have a bearing on the overall level of network security and, possibly, the range of security measures that could be implemented. Only 10% of SMBs said they would need more human resources while 12% said network security would improve if they had larger budgets.**

Computer users are the least predictable and controlled security vulnerability. In the majority of cases, a lack of education and an understanding of basic security principles and procedures are the main causes of security breaches rather than malicious activity – although the latter can never be ignored. And it takes so little for a security breach to occur.

**IT managers today have to dedicate more time and resources to deal with end-user support issues. The proliferation of consumer devices and the increasing number of employees using laptops, in and out of the office, have widened a network's footprint and with that the associated increase in threats. As the survey shows, so has the workload for IT managers in SMBs.**

#### **BUDGETS:**

From a financial perspective, spending on security measures was relatively low with 55% of SMBs saying they spent less than 10% of their IT budget on security. 38% said they allocated between 11% and 30% of the budget to security, while only 2% said they spent more than half of the budget on security.

**Despite fewer resources being allocated to security, more than three quarters of respondents were satisfied (77%) and felt that their budget was enough to cover their security requirements. However, the survey also showed that just over 50% of respondents found it difficult to convince management to invest in security solutions. Only 15% said it was very easy.**

It is likely that those who found it difficult to convince management to invest in security were trying to sell to management a solution that was not in their typical shopping cart.

**Most in senior management are familiar with the traditional security products, namely anti-virus, anti-spam and a firewall. IT managers encounter few problems purchasing these products however convincing management to spend on vulnerability management, event log management and email management and archiving solutions is another matter altogether. And this might explain why 25% feel that management needs to be more aware of security threats facing companies today.**

According to the survey, the shopping list for SMBs in the US in the coming six months includes network monitoring (31%), email management (29%), network scanning (26%) and anti-virus (26%) solutions. 15% plan to implement endpoint security or patch management (16%) solutions in the coming six months.

Ends.