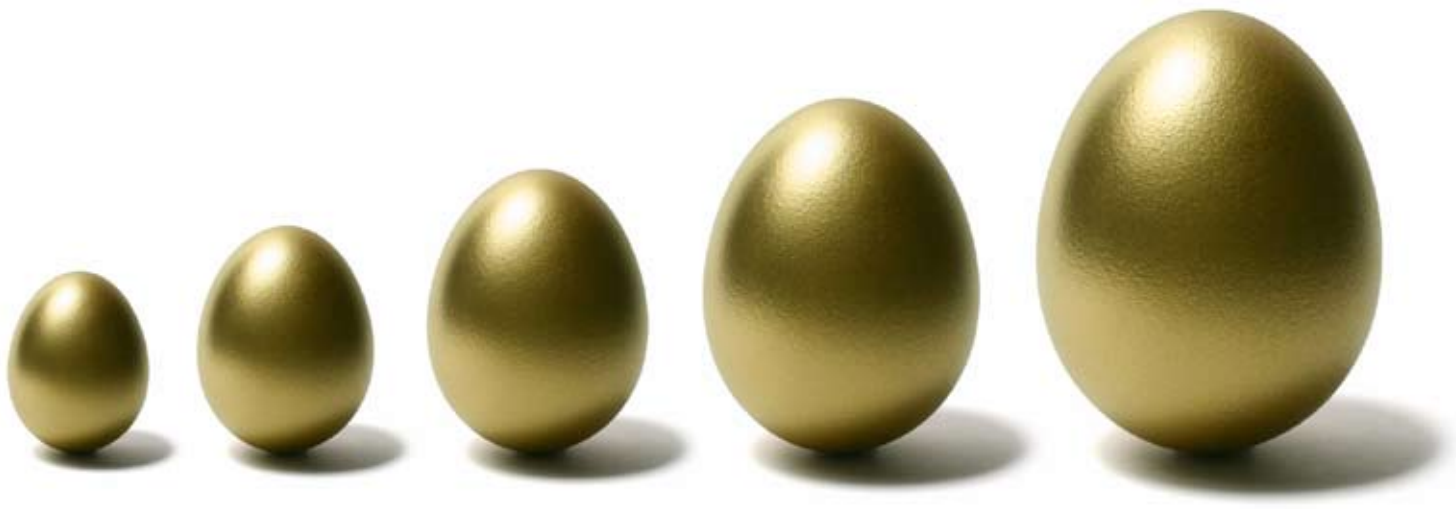
McAfee®

Does Size Matter?
The security challenge of the SMB

The First Examination into the IT Security Challenges Faced by North America's Small and Midsized Businesses



CONTENTS

Forward ..... page 3

Key Findings North America ..... page 4

Does Size Matter? ..... page 5

It Won't Happen to Me ..... page 8

False Sense of Security ..... page 10

A Question of Time ..... page 11

Size Doesn't Matter ..... page 13

North America -vs- Europe ..... page 14

Five guidelines for SMB security ..... page 15

Contact ..... page 17

Foreword

North America's 7.4 million small and medium sized businesses are operating in an increasingly competitive environment and tough economic climate[1]. They are becoming more and more reliant on the Internet to grow and succeed but are in denail about cyber security threats.

For businesses of all sizes, viruses, hacker intrusions, spyware and spam can lead to lost or stolen data, computer downtime, decreased productivity, compliance issues, lost sales and even loss of reputation. Just because a business is small, it doesn't mean it's immune to security threats.

For this report, McAfee® (www.mcafee.com) surveyed 500 companies with 2-1000 employees in the United States and Canada. The findings were then compared to the results of last year's "Does Size Matter" report, which was conducted among 600 SMBs in Europe. There is a predominant belief that SMBs on both sides of the border (and in Europe) are **too small** to be of any value to cyber criminals, and most SMBs are confident that they are **adequately protected** by default settings on their IT equipment. This is a dangerous misconception and SMBs need to understand how best to protect their business. In conducting this study, we hoped to uncover what is stopping these SMBs from moving security up on their business priority list.

We realize that fighting malicious code, hacking, spam and fending off phishing (or even SMSishing, a type of phishing attack where mobile phone users receive text messages containing a Web site hyperlink, which, if clicked would download a Trojan horse to the mobile phone) attacks can tap into the valuable resources of a small business. Our survey found that on average SMBs have **just one hour a week** to dedicate to IT Security, which is why it's important for a business to choose the right, easy-to-manage product.

Bearing this reliance on the Internet in mind, if a business does become a victim of a cyber crime attack, on average how long does it take a smaller business to recover? Our survey reveals it took a quarter of businesses (26 percent) an **entire week** to get their business back up and running from the most recent cyber attack.

Our message is that size doesn't matter wherever you are. A smaller business is just as vulnerable as larger enterprises to attacks from cyber criminals. I hope you find this information useful, we believe effective security is a great enabler for businesses everywhere.

Darrell Rodenbaugh
Senior Vice President, Mid-Market Segment
McAfee, Inc.

1 According to research firm AMI Partners, there are about 6.4 million small and medium-sized businesses (SMBs, or companies with 1-999 employees) in the United States and 953,000 in Canada while in Europe there are 25 million small and medium sized businesses.

KEY FINDINGS NORTH AMERICA

45% of SMBs do not think they are a valuable target for cyber criminals

35% of SMBs are "not concerned" about being a target of cyber crime

52% don't think they are well known enough to be a target of cyber criminals

92% claim online access and availability is important to the running of their business

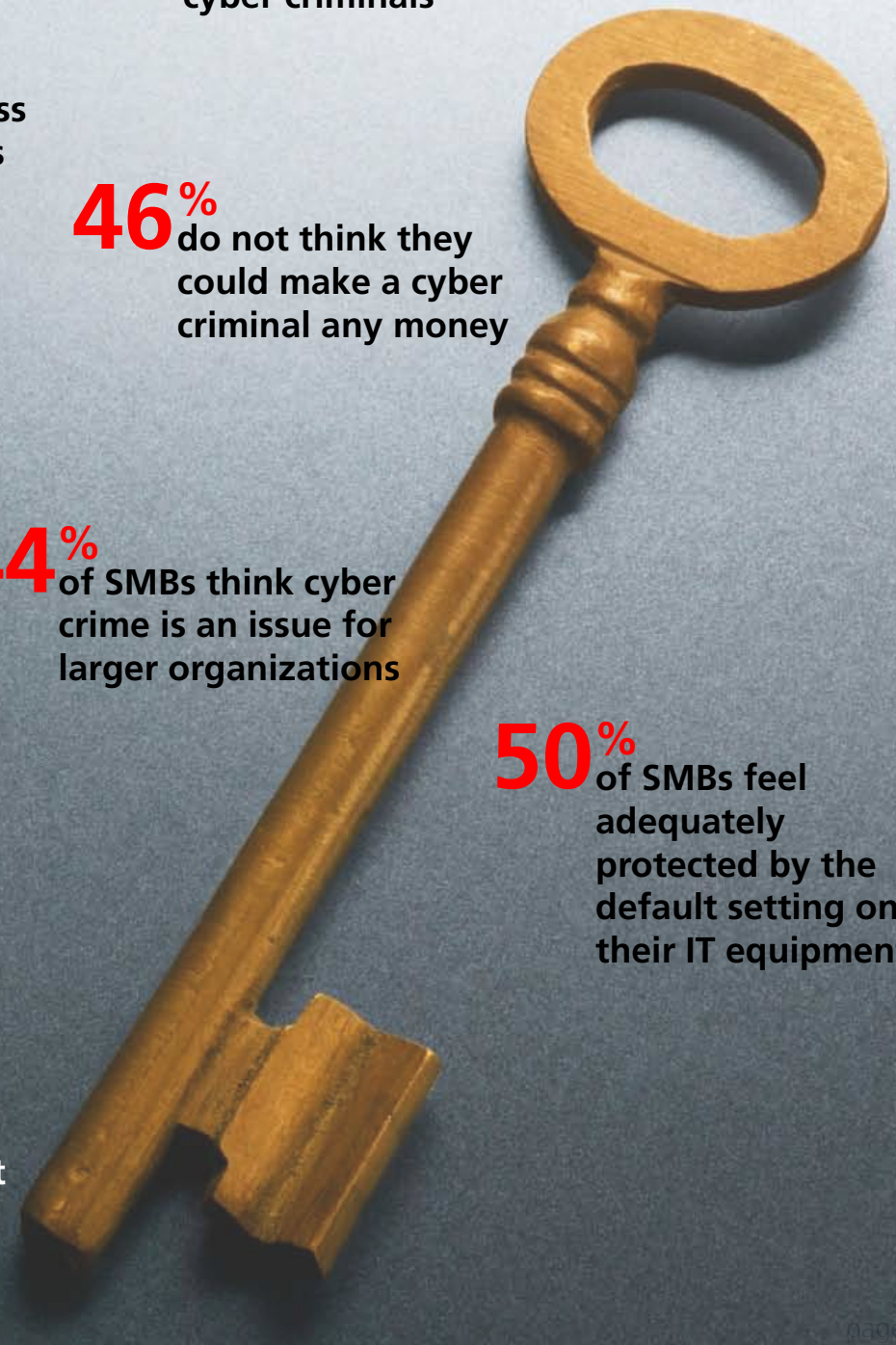
46% do not think they could make a cyber criminal any money

21% of SMBs realize a security attack could put them out of business

44% of SMBs think cyber crime is an issue for larger organizations

34% don't think their information has value outside the organization

50% of SMBs feel adequately protected by the default setting on their IT equipment



The majority of SMBs spend just one hour a week on IT Security

DOES SIZE MATTER?

Ask a cyber criminal if size matters and the answer is no, they don't care whether they target individuals, or large or small corporations.

For example, a bot herder—a hacker who installs malicious software on computers through the Internet without the owners' knowledge—all they need is a computer that can be abused for click fraud[2], sending spam etc. They have no concern about who the computer belongs to.

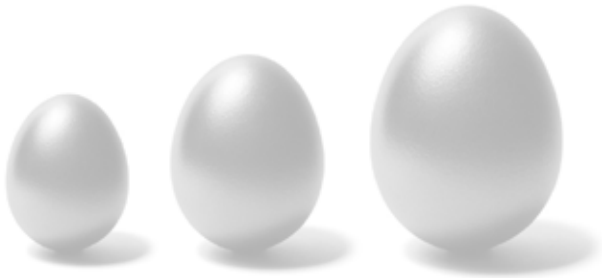
Cyber criminals and hackers cost businesses real money, according to the 10th annual 10th Annual CSI/FBI Survey released last October. In 2007, companies in the United States lost an average $350,424 a year due to cyber security incidents. This is double the average losses reported in 2006 ($168,000).

According to the businesses questioned in this study, just over **one in five (21 percent)** of businesses have suffered an IT security attack. A **third** of those businesses **(32 percent)** have suffered more than four IT security attacks in the last three years and McAfee Avert® Labs intelligence tells us attacks are increasing.

This study shows that SMBs have become very reliant on the Internet, with **92 percent** of respondents claiming that online access and availability is very important to the running of their businesses.

The downtime cost for small companies is just over $30K (0.4 percent of revenue), with medium companies topping $225K (0.5 percent of revenue) and large companies passing $30M (2.2 percent of revenue). Infonetic's report, "The Costs of Network Security Attacks: North America 2007."

According to Jeff Wilson, Infonetics Research, "Working on computers and accessing networked resources and the Internet are the life-blood of modern business, and anything that blocks access to electronic resources is crippling. Small and medium businesses lose roughly half of their revenue annually to security downtime. At medium organizations, spyware alone is responsible for a major portion of downtime costs at 47 percent and small organizations aren't far behind at 40 percent of downtime costs. Server malware is also a big problem for both of these groups."



2 Type of Internet crime that occurs in pay per click online advertising when a person, automated script, or computer program imitates a legitimate user of a Web browser clicking on an ad, for the purpose of generating a charge per click without having actual interest in the target of the ad's link

DOES SIZE MATTER?

Bearing this reliance on the Internet in mind, if a business does become a victim of a cyber crime attack, on average how long does it take a smaller business to recover? Our survey reveals it took **a quarter** of businesses **(26 percent)** an entire week to get their business back up and running from the most recent cyber attack.

Canadian SMBs were affected worse than their counterparts in the United States with **36 percent** taking one week to recover from an attack compared to **26 percent**.

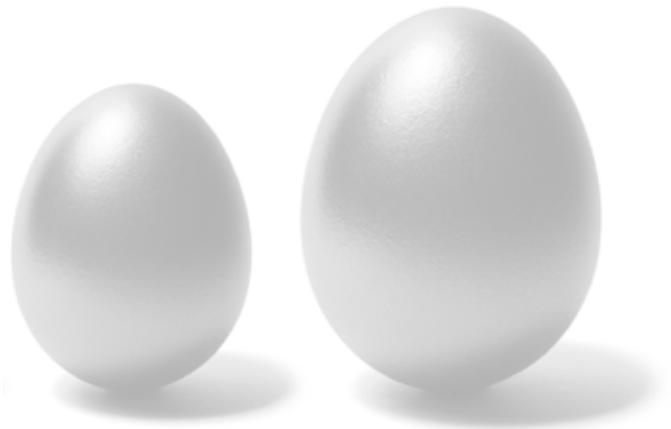
This is not a problem limited to North America. In a similar survey conducted among European SMBs, the country affected the worst was Spain, with **50 percent** of Spanish SMBs surveyed taking one week to recover.

Percentage of businesses who have taken one week to recover from an attack:

The Netherlands	6 %
Italy	15 %
United Kingdom	18 %
Germany	24 %
United States	**26 %**
France	28 %
Canada	**36 %**
Spain	50 %

In comparison to larger organizations, attacks can be even more catastrophic as SMBs often don't have the resources or funds to build contingency plans. If a resource goes down, a business often goes down with it. North America's SMBs are leaving themselves open to attack due to time constraints.

"Cyber criminals don't discriminate and to them, size doesn't matter," Jeff Green, senior vice president of McAfee Avert Labs. "In fact, high profile attacks are becoming less frequent because they are often detected more quickly, and attackers are favoring 'stealth' attacks that quietly infiltrate systems. Attackers often assume that smaller businesses will not have technology to identify their attacks and therefore regard them as easy pickings."



DOES SIZE MATTER?

Coupled with the perception that SMBs are "easy pickings", cyber criminals are increasingly turning their attention to technologies such as Voice over IP, (e.g. Skype), smartphone software (Blackberrys) and new virtual systems. These technologies are being progressively adopted by SMBs as they offer substantial cost-savings and flexibility, making SMBs even more likely to become targets.

Employees are using the Internet for social networking on the likes of Facebook and LinkedIn and the use of Instant Messenger is rapidly increasing; these technologies bring many advantages but also many more potential 'doors' through which cyber criminals can access information or infiltrate systems.

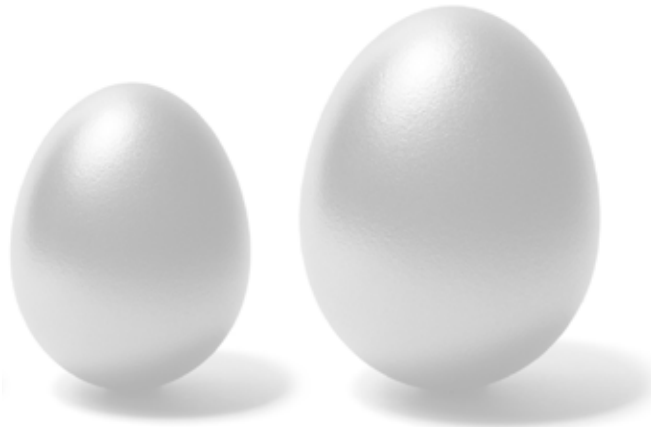
So why do so many SMBs think they aren't targets for cyber crime? From the research we know that SMBs understand the damage a breach would cause their business. Nearly **one in five** businesses surveyed felt that an IT security attack could put them out of business (**21 percent**).

According to McAfee Avert Labs' top ten predictions for security threats in 2008. Researchers at McAfee Avert Labs expect an increase in Web dangers and threats targeting Microsoft Corp.'s Windows Vista operating system, among other new or increased threats. "Professional and organized criminals continue to drive a lot of the malicious activity. As they become increasingly sophisticated, it is more important than ever to be aware and secure when traversing the Web," commented Green.

This belief is similar regardless of the size of the SMB; **17 percent** of SMBs with 2-10 people, **22 percent** of SMBs with 11-100 people and even higher in larger organizations of 101-1000 people (**29 percent**) agreed that a security breach could put them out of business.

With this in mind, why is the level of concern about actually being attacked still so low? The next few sections explore several possibilities; the 'it won't happen to me' mentality, the belief that businesses are already adequately protected and the restrictions of time pressures faced by small and mid-sized companies.

"Threats follow the money and we predict that the VOIP trend and the Web 2.0 phenomenon will continue to influence future threats," added Green. "VOIP is a particularly attractive target, given criminals can look to target both voice and data networks at the same time."



IT WON'T HAPPEN TO ME

While SMBs are concerned about the dangers of the cyber crime, this study reveals that SMBs in the United States and Canada are burying their heads in the sand, living with the belief that the smaller they are the less of a target they are to cyber criminals.

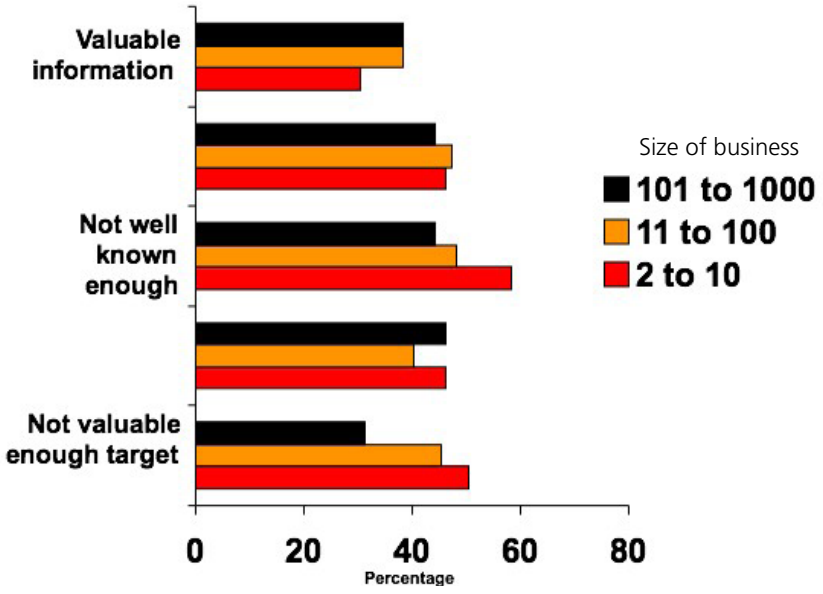
The strongest opinion from **over half** the SMBs from North America was that they do not think they are 'well-known' enough to be on a cyber criminal's radar with **52 percent** of respondents citing this response. This was closely followed by the belief that they didn't have enough information to make a cyber criminal any money (**46 percent**). **Almost half** (**45 percent**) believed that they weren't a 'valuable enough target' and that cyber crime was an issue for 'larger' organizations (**44 percent**). **Over a third** of respondents also answered that they didn't think they had any information that would be valuable to people outside the organization (**34 percent**).

In Europe, the strongest opinion from over half the SMBs is that they do not think they are a 'valuable enough target' with **58 percent** of respondents choosing this response.

"Almost any small business, even the very small ones with less than five employees, will at the very least have some stored records of confidential customer and employee information that would be of use to a cyber criminal, especially to commit crimes like identity theft," said Rick Jackson, director of North American small business at McAfee.

As the term SMB covers a huge range of organizations, it could be assumed that businesses towards the larger end of the spectrum would fall way below these percentages. However, our study has found this is not the case; **44 percent** of organizations with between 101-1000 employees agreed that they weren't well-known enough and **44 percent** stated that they wouldn't have information that would make a cyber criminal any money, almost a third (**31 percent**) said they aren't a valuable enough target, almost half (**46 percent**) felt that cyber crime was an issue for larger organizations and **s**thought didn't think they had any information that would be valuable to people outside the organization. See graph 2.

Graph 2: Reasons why businesses don't feel they are a target for cyber criminals.



IT WON'T HAPPEN TO ME

Most popular reasons across North America and Europe why SMBs do not think they are attractive targets to cyber criminals

We don't have any valuable information to people outside our business

Germany	21 %
Canada	**32 %**
United States	**34 %**
The Netherlands	37 %
France	37 %
Spain	40 %
United Kingdom	42 %
Italy	44 %

Cyber crime is more of an issue for larger organizations

Germany	26 %
The Netherlands	36 %
Canada	**44 %**
United States	**44 %**
United Kingdom	47 %
Spain	51 %
France	59 %
Italy	65 %

We don't have sufficient information to make a criminal any money

Canada	**46 %**
United States	**46 %**
Germany	46 %
The Netherlands	47 %
Spain	53 %
United Kingdom	54 %
France	62 %
Italy	71 %

We are not a valuable enough target

Germany	42 %
Canada	**45 %**
United States	**49 %**
France	51 %
United Kindgom	57 %
The Netherlands	59 %
Spain	67 %
Italy	74 %

FALSE SENSE OF SECURITY

In addition to not believing they are 'valuable' or 'well known' enough targets for cyber criminals, another reason for the low level of concern comes from the fact that smaller businesses feel they are protected from potential threats.

Our survey established that **20 percent** of businesses felt very protected and a further **68 percent** had some form of protection. What is surprising is that over **one in five** businesses had a little or no protection.

One would expect the larger the organization, the more they would be protected and feel secure. Surprisingly it was the opposite; organizations between 2-10 people felt more protected (**22 percent**) than people in organizations of 101-1000 (**17 percent**).

However, these figures don't show the sophistication of security precautions – it could just mean simply using passwords to protect systems and hardware, which unfortunately is not enough to stay safe.

While the perception of these businesses is that they are adequately protected, our research reveals that **half** of the SMBs (**50 percent** of SMBs in the United States and **45 percent** of SMBs in Canada) surveyed trust the default settings on their IT equipment and **almost half** (**43 percent** of SMBs in the United States and **46 percent** of SMBs in Canada) typically accept the default settings.

"Simply using the default settings is a dangerous practice," comments Jackson. "It gives SMBs a false sense of security as they think they are protected. Simply using the recommended settings isn't enough given the complexity and ever changing security threats. Default settings are freely available to cyber criminals, which means that it doesn't take them long to find ways to crack the security settings "gaps" and infiltrate a business systems and networks, without the owner even knowing his confidential data is compromised.

Percentage of SMBs most likely to accept default setting on their IT equipment

Germany	20 %
United Kingdom	35 %
Italy	35 %
France	36 %
The Netherlands	38 %
United States	**43 %**
Canada	**46 %**
Spain	50 %

In terms of size, there is little difference of opinion regarding defaults. In fact the businesses towards the larger end of the spectrum of SMBs (101-1000) scored higher than the average with **55 percent** agreeing that the default settings provide adequate protection, compared to **43 percent** of businesses with 11-100 people and **54 percent** of businesses with 2-10 people.

A QUESTION OF TIME

This research confirms that one of the reasons that SMBs are not concerned with security is simply a matter of time.

"SMBs are the least protected and the most exposed", according to Jackson. "Many small businesses are aware that they need to protect themselves against IT security threats but they don't have the time to invest in managing all the emerging threats, keeping systems updated, nor the IT budgets to buy and maintain complicated, expensive security solutions," explains Jackson. "It's a constant challenge to balance the resources available in comparison with the perceived threat."

According to a recent IDC study, SMBs are driving the bulk of all IT sales in the United States.

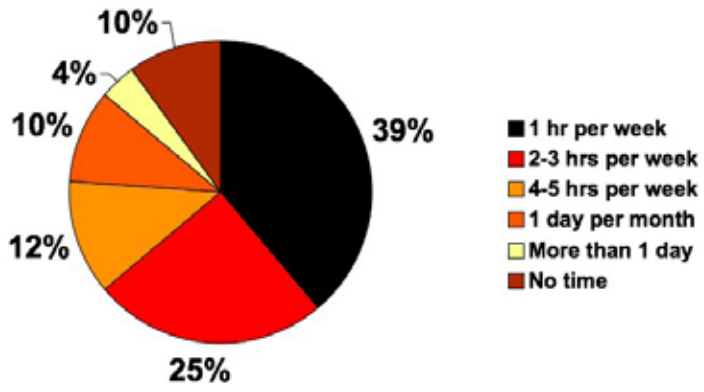
A recent Everything Channel Survey of SMB End Customers in April 2008 reported that IT for the SMB is a $270 billion market. The biggest opportunities are telecom equipment and service ($73 billion or 27 percent) and IT services ($68 billion or 25 percent). Next comes Computing ($56 billion or 21percent) and Internet ($29 billion or 11 percent) and then Software ($24 billion or 9 percent). Lagging behind is networking/security/ storage ($19 billion or 7 percent).

As previously mentioned SMBs understand that a serious security breach would harm their business, but other priorities – often to keep the business alive – are simply more pressing. It is therefore undeniable that lack of time is a concern when it comes to IT security for smaller and mid-sized businesses.

Our research shows that time constraints mean that the majority (**39 percent**) of businesses surveyed in the United States spend just one hour per week on proactively managing IT security threats. More Canadian businesses spent just one hour per week (**44 percent**).

"Time constraints are definitely a contributory factor to SMBs security. In focus groups, SMBs have told us that they don't have enough time and they would rather not do anything rather than give it to someone else to do," said Rodenbaugh. "One of the most effective options for an SMB is to buy security-as-a-service."

Percentage of time spent proactively on IT Security



A QUESTION OF TIME

Time spent proactively on IT security by country

One hour per week

Italy	13 %
Spain	21 %
The Netherlands	27 %
France	30 %
United Kingdom	33 %
United States	**39 %**
Canada	**44 %**
Germany	45 %

Half a day per week

Germany	7 %
Italy	8 %
The Netherlands	8 %
Spain	8 %
Canada	**9 %**
United States	**12 %**
United Kingdom	13 %
France	15 %

One hour per day

Canada	**9 %**
United States	**12 %**
France	13 %
United Kingdom	17 %
Germany	22 %
Italy	25 %
The Netherlands	28 %
Spain	28 %

One day per month

United Kingdom	3 %
France	6 %
Germany	7 %
Spain	7 %
The Netherlands	13 %
Italy	23 %
United States	**25 %**
Canada	**26 %**

One day per week

Canada	**7 %**
France	7 %
The Netherlands	8 %
United Kingdom	9 %
Germany	9 %
United States	**10 %**
Italy	14 %
Spain	21 %

SIZE DOESN'T MATTER

In answer to our initial question; Does size matter? The answer to this is no. Not in the world of cyber crime.

It doesn't matter to a cyber criminal how big or small your business is and smaller businesses are just as lucrative targets as larger ones for IT security attacks.

Today's attackers focus on the type of application used to achieve their attack, in many instances both SMBs and enterprises use the same applications.

SMBs can become victims of viruses, hacker intrusions, spyware, spam and even ransomware leading to stolen data, computer downtime, decreased productivity, lack of compliance, lost sales and loss of reputation.

An attack focused on an SMB will often be for a smaller amount (and will therefore be below the radar of organizations like the FBI, who focus on larger crimes), but lots of small attacks add up to large amounts of revenue.

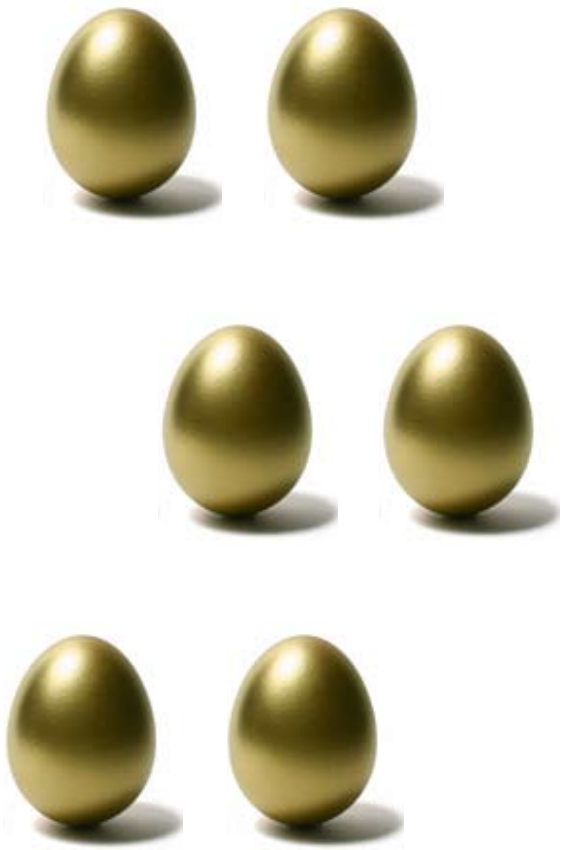
Unfortunately, in terms of available time and resources size often means smaller businesses can't dedicate the time they would like to fully managing potential threats and intrusions.

McAfee's vision is for security to be a growth enabler, not just a necessary defensive measure. Our 200 researchers based around the world are constantly working to identify current and future threats and counter the increasingly sophisticated nature of cyber crime. We want to challenge and uncover these misconceptions to put SMBs in a safer place – ready to safely employ technologies that will help them achieve their goals.

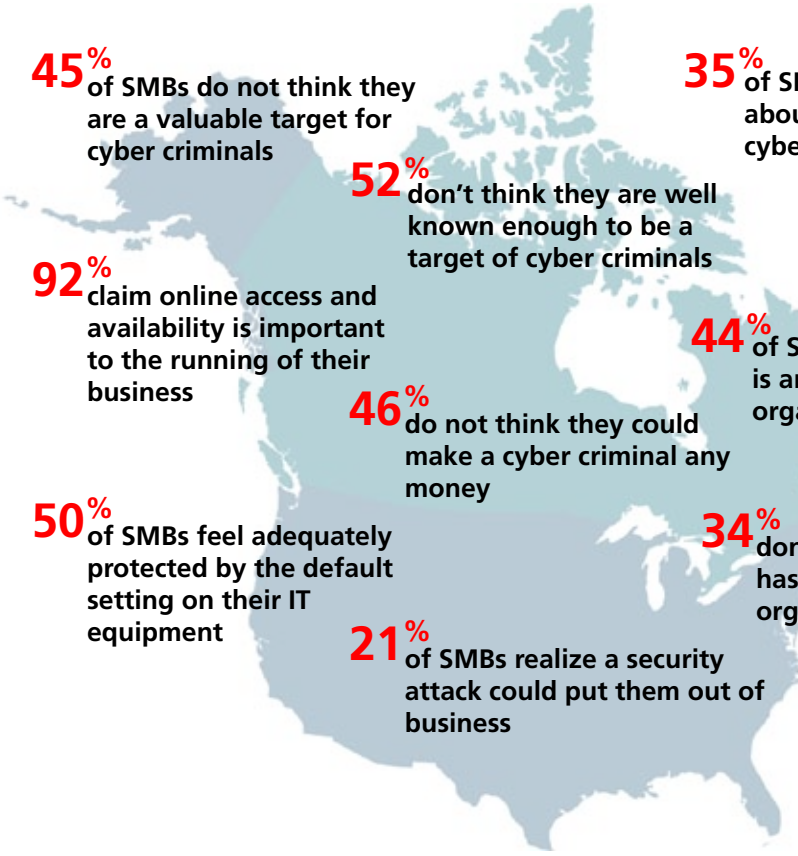
"In an ideal world we'd all be 100 percent protected, but the cyber criminals move at such a pace and time constraints means that this just isn't feasible", comments Rodenbaugh.

"We encourage small and medium sized businesses to look closely at their most valuable assets – what matters to them most - and ensure that those assets are protected. For one business it might protecting their customer database, for another it might be safeguarding intellectual property and ideas, and yet for another it might be securing their financial information."

Rodenbaugh continues, "For an SMB, the best choice is to choose one solution that covers the most likely threats to their business."



NORTH AMERICA -VS- EUROPE



45% of SMBs do not think they are a valuable target for cyber criminals

52% don't think they are well known enough to be a target of cyber criminals

92% claim online access and availability is important to the running of their business

46% do not think they could make a cyber criminal any money

50% of SMBs feel adequately protected by the default setting on their IT equipment

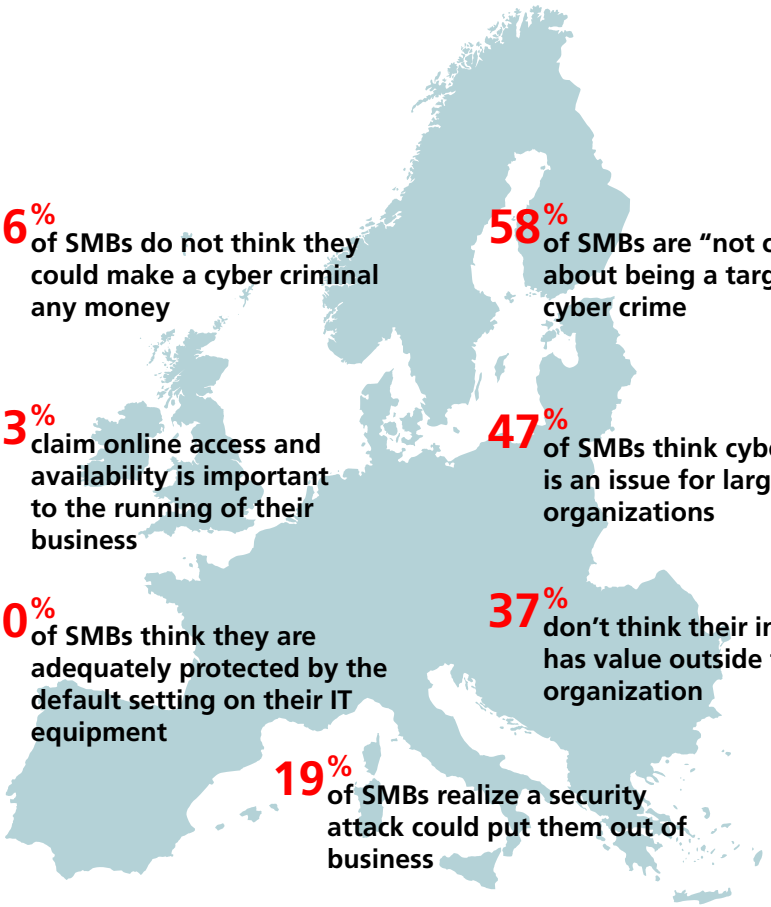
21% of SMBs realize a security attack could put them out of business

35% of SMBs are "not concerned" about being a target of cyber crime

44% of SMBs think cyber crime is an issue for larger organizations

34% don't think their information has value outside the organization

The majority of North American SMBs spend just one hour a week on IT Security



56% of SMBs do not think they could make a cyber criminal any money

73% claim online access and availability is important to the running of their business

90% of SMBs think they are adequately protected by the default setting on their IT equipment

19% of SMBs realize a security attack could put them out of business

58% of SMBs are "not concerned" about being a target of cyber crime

47% of SMBs think cyber crime is an issue for larger organizations

37% don't think their information has value outside the organization

FIVE GUIDELINES FOR SMB SECURITY

Security doesn't have to be Complicated
SMBs need protection that is simple to install and easy to maintain at current levels of protection. Time should be dedicated to the success of their business, not the constant safeguarding of the network. SMBs can implement the following security best-practices to protect their business.

- Create a business security policy and train employees to follow the procedures Establish clear company policies about downloading music, pornography, chat room or gaming applications.
- Practice good password and account protocols
- If an employee does not need the software application for legitimate business purposes, don't load it on their computer
- If the business is not using software or ports, disable them
- Maintain security patches. These patches will give SMBs the most up-to-date security protection. SMBs can also subscribe to a managed security service that does the work for them. Their security is only as good as the last update.
- Seek security solutions that are easy to use and quickly deployed
- Seek security solutions that have "built-in" intelligence and default configurations and policy settings so they can leverage the industry best practices

Smart Security is Proactive, not Reactive
An ounce of prevention is worth a lot more than ton spent on cure. On average, the cost of preventive measures is four times less than the cost of a data breach for businesses. The key is to find a security solution that could help SMBs avoid these costly breaches and threats.

- Keep abreast of the latest security trends by subscribing to feeds such as Security Insights
- Be sure to encrypt laptops and mobile devices such as USB sticks, as they could avoid leakage of sensitive employee, customer or company information and avoid costly breaches and law suits
- Proactively block employees from accessing bad or malicious Web sites with technologies such as SiteAdvisor™ built-in to their security solutions
- Look for an antivirus solution that not only goes beyond detecting known viruses, but also stops unknown threats on their tracks
- Filter spam from email even before they get to the network
- Look for a solution that alerts users to security issues and either automatically takes the right security actions or guides the user through an intuitive management console

FIVE GUIDELINES FOR SMB SECURITY

Don't Sacrifice Security Based on a Limited Budget

Many SMBs can't always afford a specialized IT security staff member or the time and resources to be taken away from business-critical priorities.

- Seek affordable and proven technology
- Try to avoid putting in piece-meal technologies. With threats becoming more integrated, SMBs should look for solutions that stop multiple threat vectors
- Prioritize security based on business needs. For instance, if a business is a retailer doing a majority of its business online, it is more important for them to ensure their Web site is secure and hacker-safe. Likewise, if the business is a law firm or local bank, stopping theft of sensitive data is more critical
- Install and routinely update desktop anti-virus, using solutions that are proactive in identifying and deleting known and unknown viruses
- Subscribe to a managed security service and add layers of protection based on business priorities and budget

Networks are becoming Increasingly Permeable

Securing employees' use of the Internet, extranets and intranets has never been so important. In addition, there are an increasing number of options for remote connectivity to critical applications, making businesses more vulnerable to unauthorized access.

- Remote users represent a major challenge to protect; they frequently have low-bandwidth connections, are often inaccessible to network administrators and may not have updated virus protection
- The potential for a virus infection exists anytime an executable file or document is transferred using FTP or users sharing files
- Internal threats (e.g., employees) are reported to be among the top-root sources of malicious activities
- Look for solutions that can provide protection both against internal and external threats across your network

E-Mail Security is a Threat, not just a Nuisance

One of biggest threats to SMBs is a virus that arrives as part of an e-mail. Identify business-specific rules that can be applied to e-mail entering the network to help determine what is safe to reach the end user or what could be a potential threat. Also be wary of the type of outbound messages sent. Those containing offensive comments about race, gender or sexual orientation can create legal liabilities. Sending an e-mail is like mailing a postcard, many people can read it along the way.

- Provide users with a company e-mail usage policy
- Don't share e-mail addresses and don't open e-mails from unknown sources
- Don't double-click attachments unless the user knows what they are and do not open anything with a double file extension (e.g., hello.txt.vbs)
- Implement free safe searching tools, such as McAfee SiteAdvisor
- Ensure you have anti-spam measures in place
- SMBs can improve productivity and protect their business by filtering and cleaning e-mails before even they even reach the network, distract employees and impact business
- Mitigate inappropriate content by automatically adding a disclaimer message to all outgoing e-mail
- Prevent inappropriate, unsolicited or hostile messages and files through content filtering

For more information on **McAfee®** solutions available for SMBs, please visit www.mcafee.com

Research Methodology

The research for the North American study was conducted this year by MSI, questioning 500 IT decision makers in organizations located in Canada and the United States with between 2 and 1000 employees. The research for the European study was conducted in 2007 by ICM Research with 600 IT decision makers in organizations of the same size in the UK, France, Germany, The Netherlands, Italy and Spain.

Detailed breakdowns are available on request.

For more information please contact:

United States
Tracy Ross
McAfee, Inc.
(408) 346.5965
tracy_ross@mcafee.com

Canada
Kathy Swail
McAfee, Inc.
(514) 830.5776
kathy_swail@mcafee.com