

## WHITE PAPER

---

# SMBs in a Connected World: Business Success Means Facing New IT Security Threats

MessageLabs and McAfee

---

Eric Damage

Robert Redgate

Phil Odgers

January 2007

## IDC OPINION

In a piece of primary, global research recently conducted by IDC it was clear that small to medium sized businesses (SMBs) are increasingly reliant on IT and the Internet/Web for company communications, operational effectiveness, and reaching their defined business objectives. These business objectives are naturally focused on such things as increased profit and revenue, but significantly, IT security (ITS) was a top business priority for only 8% of the SMBs that took part in the research.

This figure is significant in that the vast majority of SMBs think that a serious breach in ITS would be very detrimental to their ability to achieve their stated business objectives. This view is compounded by the fact that the same SMBs perceive that an inability to achieve these stated business objectives would have a very negative effect on the company's overall health and wellbeing.

All of the above stacks up to indicate that there is evidently a very straight road linking IT security to the business health and success of the SMB community. In fact, for the unfortunate ones in the research that had experienced an ITS breach, a solid majority reported a bad negative effect (or worse) on their commercial operations, with very few reporting only a minor effect.

Despite this clearly defined situation, very few SMBs are overtly proactive in their fight against an ITS breach. Most take a tactical, reactive positioning and seem to be preoccupied with "keeping the shop open for business" rather than thinking strategically with an eye to the future threats that are coming their way.

So, despite a clear understanding of the current ITS threat and its potential effect on the well-being of the company, there is a serious commercial threat emerging within the SMB community. IT professionals do not appear to be analyzing future potential risks or rather do not have the time to consider those risks due to the time-consuming nature of their tactical ITS activities and/or the limited resources that they have to apply to the task.

**This raises the question, "How can SMBs face present and future threats while being occupied by daily tasks?"**

In response, IDC would contend that managed security services (MSS) provide an effective and responsive answer to the dilemma in the SMB community. In fact, one of IDC's top 10 predictions for the ITS market in 2007 states that the commoditization of ITS functionality will drive a shift to ITS-based services. IDC believes that 2007 will see a continuance of the global shift from PC- or LAN-based software security solutions to flat-rate security services outside the LAN.

For a more detailed response to this question, readers should consult the sections at the end of this paper headed "IDC's Recommendations for SMBs" and "Future Outlook."

## **METHODOLOGY**

These findings are based on the results of 450 interviews with SMBs across the United States, the UK, Germany, and Australia. The interviews were undertaken in November 2006 and all respondents were responsible for, or actively involved in, the IT decision-making process for their organization.

The organizations that were interviewed varied in size from a minimum of 80 people employed to a maximum of 250 people. The following vertical industries were chosen for interviews:

- Professional services
- Business services
- Manufacturing
- Financial services
- Banking
- Media and marketing

## **IN THIS WHITE PAPER**

This white paper provides a discussion on ITS and how it affects the ability of SMBs to protect their businesses, and associated business objectives, from both external and internal IT-based threats. The focus of this paper is to give executives and senior decision makers an understanding of the situation that currently prevails within the SMB community and how they might best protect their company and its interests from computer-related threats.

## SITUATION OVERVIEW

### The Extent to Which SMBs Rely on IT and the Internet/Web

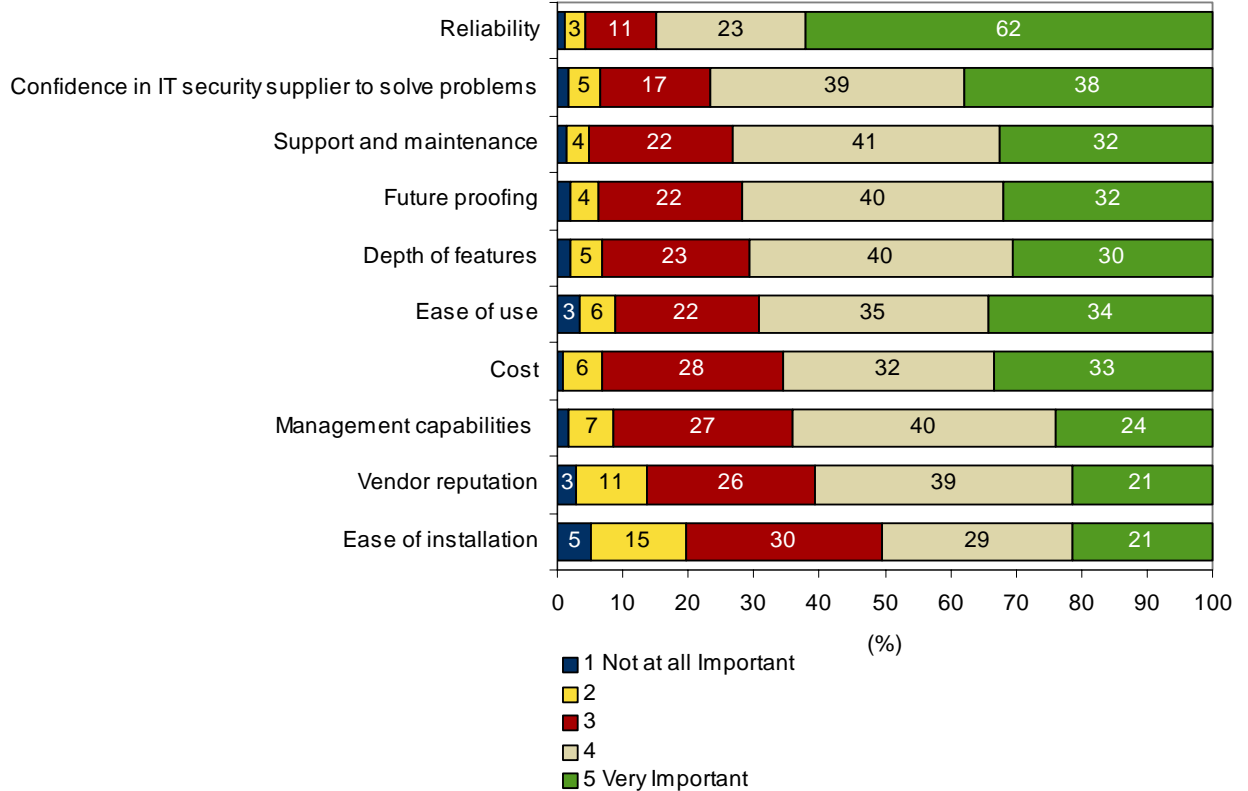
The Internet/Web is widely used by SMBs to develop their businesses and to achieve business priorities, with 90% of research respondents active or semi-active users and only 1% appearing not to use the capability at all. In particular, the Internet/Web is widely used for communication needs (e.g., their image) of the SMB community, with the US and UK being prominent at a country level with this means of communication. As part of this usage, email is widely used by the SMB community's employees to conduct its business, with 87% of employees using the capability.

This level of usage means that, inadvertently, SMBs are becoming increasingly reliant on the reliability, reputation, and support of companies that provide ITS software and associated capabilities. The view of SMBs towards these companies is clarified in Figure 1.

**FIGURE 1**

#### Use of IT and IT Security Criteria When Choosing Solutions

*When choosing a new security product or solution, what are the areas that matter to you most?  
(Please answer on a scale of 1 to 5, where 1 is not at all important and 5 is very important)*



Source: IDC, 2007

These responses indicate that SMBs believe that the perceived reputation of an ITS vendor in key areas is paramount in their choice of the new product or solution that will provide critical support to their business and the achievement of its business objectives. In this way, IT is viewed by SMBs as a stepping-stone for reaching business objectives (e.g., developing the business and its image, securing assets etc.). This is a tactical point of view.

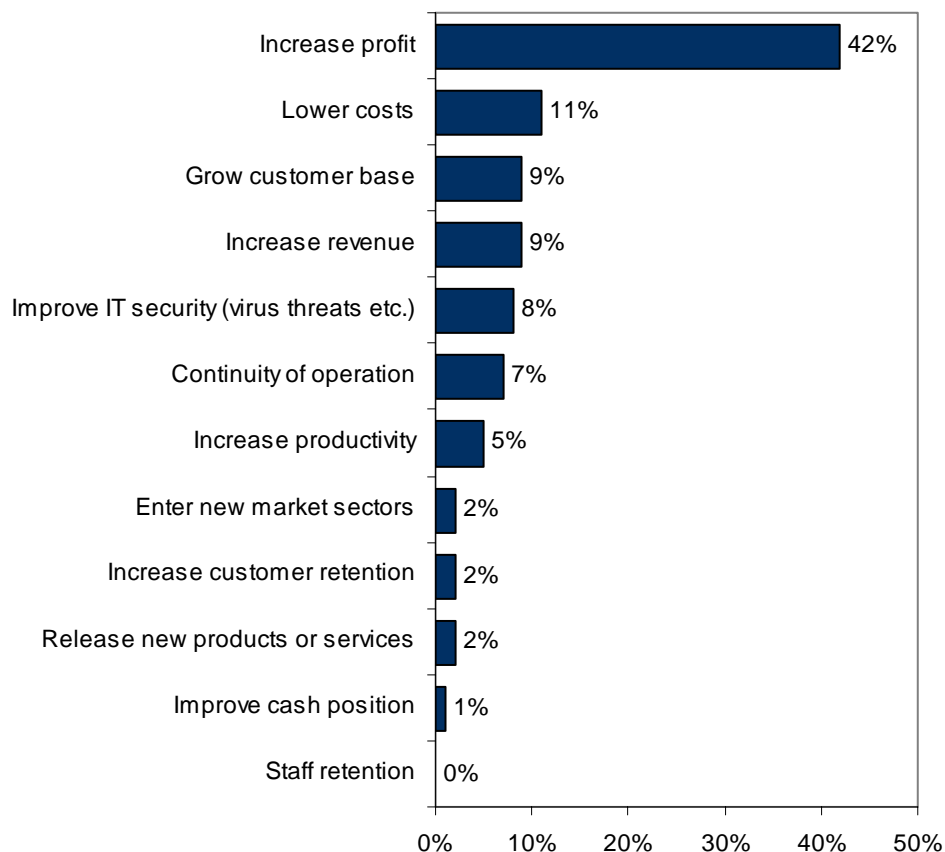
### SMB Business Focus

As one might expect, the primary business priorities for SMBs are associated with matters such as "Increase Profit," which was cited by 42% of SMBs as their top priority. The next three cited as top priority were "Lower Costs", "Grow Customer Base," and "Increase Revenue", coming in with 9% to 11% of SMBs. "Improve IT Security" as a top business priority was mentioned by only 8% of respondents in the survey, as Figure 2 shows.

**FIGURE 2**

#### Top Business Priorities

*What are your organization's 5 top business priorities and please can you rank them in order of importance?*



Source: IDC, 2007

IDC research indicates that company size plays a very important role in the view that senior management have of security. This is particularly the case with senior IT management where "Top 500" enterprise CIOs, for instance, place ITS at a much higher level of importance than is obviously the case with SMBs.

Senior IT professionals in SMBs appear more "business-oriented" than enterprise CIOs and appear to be highly involved in the company's daily business achievements. They consider ITS to be a tactical vehicle that will help them reach company goals. In contrast, regulatory pressures and strategic issues tend to isolate enterprise CIOs from the daily operations activity of the enterprises that they serve.

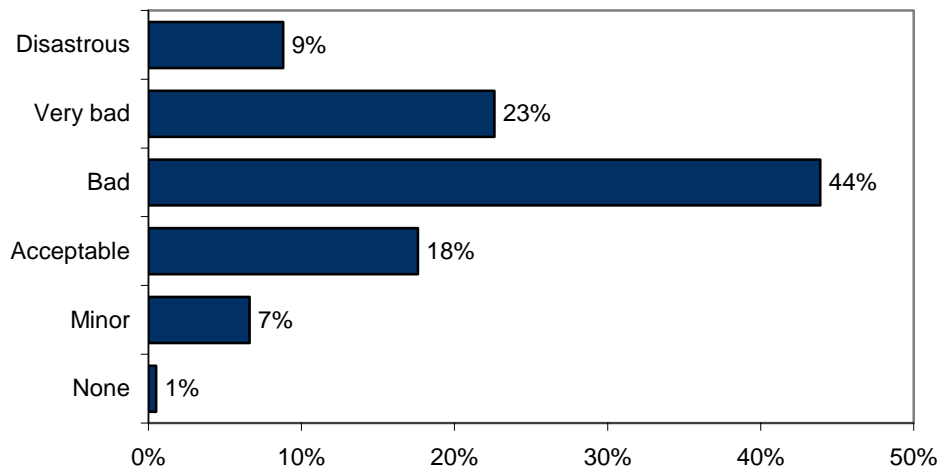
### **The Perceived Effect of SMBs not Achieving Their Stated Business Objectives**

SMBs are very aware of the negative effect of not achieving business objectives on the overall health of the company, as Figure 3 clearly shows. 76% believe that not achieving their business objectives would have a bad (44%), very bad (23%), or disastrous (9%) effect on the SMB's business. This negative effect appeared to have particular emphasis in the US and Australia.

**FIGURE 3**

#### Business Objectives

*What would be the level of effect on the organization if these priorities were not met in full?*



Source: IDC, 2007

To add emphasis to this serious position, for the respondent group the relationship between objective achievement and corporate health appears to be quite sensitive, with 47% believing that there would be a negative effect on the SMB if only half of the company's business objectives were met. To add complexity to this sensitive position, 53% of the SMBs interviewed were obliged to comply with mandatory regulations, particularly in Germany. 82% of those that have to comply stated that failure to maintain compliance, for any reason, would result in a negative effect on their ability to achieve their stated business priorities. In fact, 21% stated that the effect on their business priorities would be disastrous.

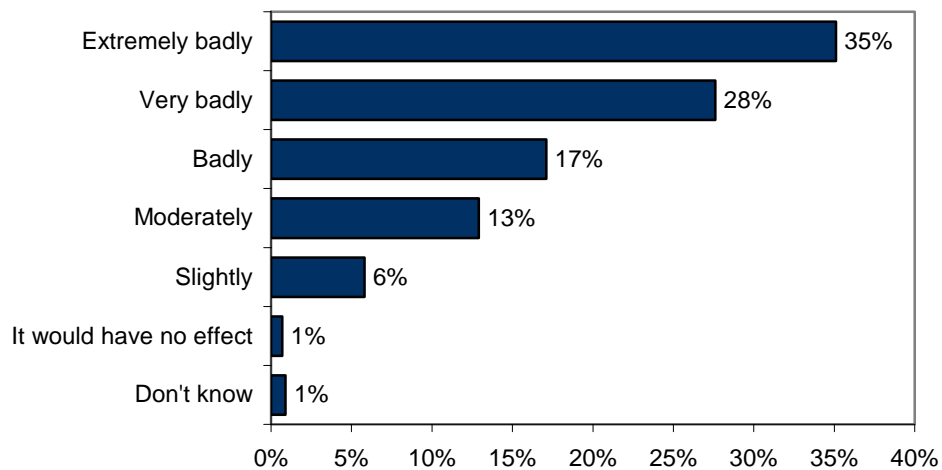
Linking this sensitivity with ITS, there is a very clear link between the two, as Figure 4 below displays. 80% of survey respondents thought that a serious breach in IT security would be detrimental to the SMB's ability to achieve its stated business priorities. In terms of how badly it would affect them, 35% said "extremely badly," 28% said "very badly," and 17% said "badly." Only 1% said that a breach in IT security would have "no effect." This link was displayed most prominently in the US, Germany, and Australia.

**Given the above results, there is evidently a very straight road linking ITS to the business health and success of the SMB community.**

**FIGURE 4**

Business Objectives 2

*How do you think that a serious breach of IT security would affect the organization's ability to achieve its stated business priorities? (E.g., If a virus knocked out all IT capability in the organization for a week)*



Source: IDC, 2007

---

## The Actual Effect of an IT Security Breach on an SMB's Business

Probably the most surprising result in the primary research is that only 18% of SMB respondents reported that they had had an ITS breach in their company. This figure was relatively consistent across all four countries where the survey was conducted, with the lowest responses in Australia (16%) and highest in Germany (21%). Given the ongoing research of IDC and others (e.g., the Department of Trade and Industry in the UK), this is a very low figure. Given the size and nature of the research, IDC believes that two possible reasons for the low figure are:

- ☒ SMBs do not wish to talk about their pain points and perceived failure — most (81%) of the respondents were personally in charge of the IT function in their company.
- ☒ SMBs do not know that they are being attacked by the new generation of ITS threats, e.g., silent (undisclosed) criminal attacks on the information assets of the company. **This possible reason is particularly serious, if true.**

For those that had experienced a security breach, the result of an attack was, for the most part, difficult for the company to say the least. 58% stated that the breach had had a bad negative effect (or worse) on their commercial operations with 31% stating that there was a detrimental effect, but that the effect was considered "acceptable." Only 11% stated that the effect was "minor" or "none" (1%).

---

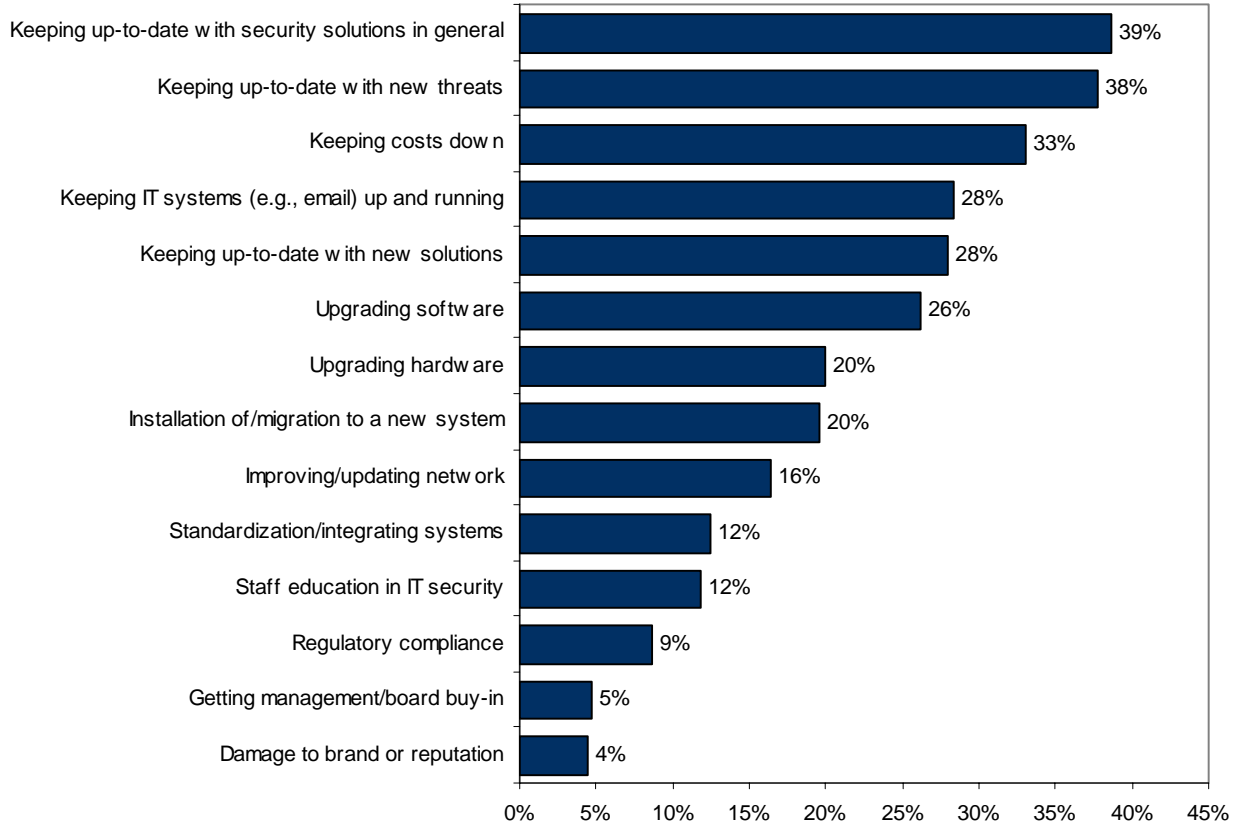
## SMB Fears, Reactions, and Pro-actions

One of the most informative results of the research is that SMB operational priorities for ITS are mainly reactive, even if the respondents believe they are "somehow proactive." In fact, only 13% of SMBs regarded themselves as being "strongly proactive" in response to the understood ITS threat. Perhaps not unreasonably for a small company, SMBs seem preoccupied with "keeping the shop open" in response to their ITS challenges. This preoccupation is shown in Figure 5.

**FIGURE 5**

Use of IT and IT Security

*From an IT security perspective, what is the biggest challenge facing your organization over the next 12 months?*



Source: IDC, 2007

"Keeping" tasks (e.g., "keeping up-to-date with new solutions") are considered by IDC to be low added value. These tasks seem to monopolize a major part of the SMB IT professional's mindset and their perceived fears are "classical" — that is outside threats such as viruses in emails. This situation is simply not sustainable when one can appreciate that these tasks can be easily outsourced.

Contrary to the SMB situation described above, ITS industry professionals forecast a major threat evolution based on:

- The classic outside threat (viruses, spam, etc.) is now easily mitigated by the ITS vendor's technology.
- Remote and distant access can easily be secured by VPN or VLAN solutions.
- The main security questions are being asked by the weakest element of the security chain — the end user.

**IDC believes that SMBs can probably face the prevailing IT risk, but they might not be prepared enough for the future needs of business protection.**

---

## Are SMBs Potentially Just the Victims of IT Security Threats?

The answer to this question is probably "No." The reasons being:

- SMB IT professionals understand and are very aware of the dangers of IT;
- SMB IT professionals fear the large, negative commercial impact of an ITS breach.

To respond to this difficult combination of understanding and fear, IT professionals in the SMB community are predicting strong growth in ITS spending over the next 12 months, with over 90% stating that they will spend more on ITS during 2007. This increase in SMB ITS spending is likely to be 20% over 2006 figures, with the US and Australia being the most "bullish" with their spending plans. Disappointingly, the same IT professionals are stating that their total IT spend will increase by approaching 30% next year, which asks the question "Is ITS being taken seriously enough as part of the IT mix?"

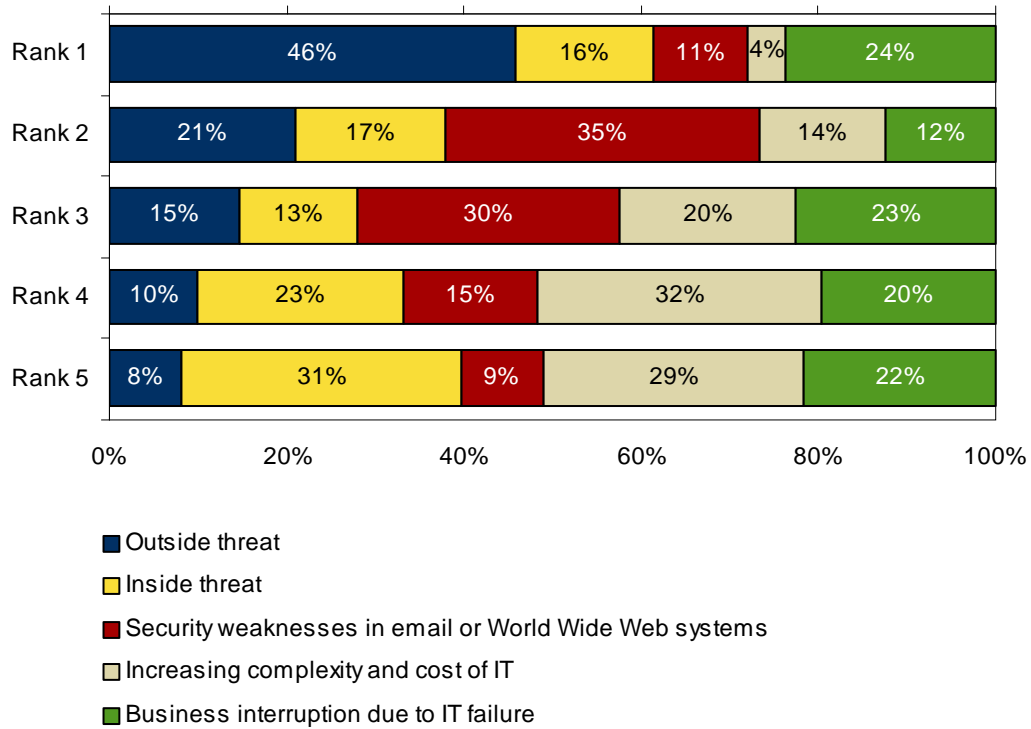
Despite the recognition and increased spending, there is a serious threat emerging within the SMB community. Present viewpoints, behavior, and spending are tactical (simple protection), but IDC believes that the future impact of any IT breaches will directly affect the core capabilities of the SMB's business. By this, we mean that financially oriented attacks will bring strong pressure on an SMB's business capacities by targeting IT assets, operational assets, and information assets (intellectual property, internal processes, strategic plans, clients databases, etc.)

This analysis of the situation is supported by the perceived threats that are feared by SMBs. These are shown in Figure 6, where respondents were asked to rank their five top fears, which turned out to be primarily tactical in nature. From this response, SMBs' IT professionals do not appear to be giving sufficient weight to analyzing future potential risks such as insider threat management or silent attacks on information value.

**FIGURE 6**

**Use of IT and IT Security: Threats**

*When thinking about all of your IT operations and assets (servers, PCs, software, etc.) please can you rank your fears about the following threats from the most dangerous to the least dangerous?*



Source: IDC, 2007

**The Main ITS Question Facing SMBs**

The ability of SMBs to face the current ITS threat is a good thing. Also, having a tactical response to protect business operations is a good thing.

**BUT...**

Activities focused on operational issues cannot give SMBs time to analyze IT threats and develop an information management strategy. Therefore, the pertinent question is:

**How can SMBs face present and future threats while being primarily occupied with daily tasks?**

---

## **IDC's Recommendations for SMBs**

One of IDC's top 10 predictions for the ITS market in 2007 states that the commoditization of ITS functionality will drive a global shift to ITS-based services. IDC believes that 2007 will see a continuance of the global shift from PC- or LAN-based software security solutions to flat rate fee security services outside the LAN.

IDC consider that Managed Security Services (MSS) provide an effective and responsive answer to the situation in the SMB community. Through this solution:

- MSS providers take on the relocation of risk management to their own ITS assets. They can afford the best ITS technologies and experts and share the cost across all of the provider's customers.
- MSS providers can provide shared analytical competencies.
- MSS providers can assume an SMB's strong motivation for business continuity by:
  - Assuming daily, low-value ITS tasks (updating, monitoring, etc.) with the best technology
  - Help an SMB's IT professionals stay focused on strategic issues rather than tactical issues
  - Help SMBs to face additional and evolving threats

## FUTURE OUTLOOK

IDC invites SMB IT professionals to take some time from their day-to-day activities and consider their current position with regard to ITS. It is IDC's opinion that:

- They mitigate daily IT risk with considerable agility, but spend all their time on this single activity.
- They are facing new threats that will directly impact their business capabilities and business objectives.
- They can afford a budget increase for their ITS facilities.

IDC believes that SMB IT professionals, through their involvement in the company's operational planning, must think about building an effective, future-proof IT security policy. This policy should respond to the following seven questions:

1. What are the company's business priorities?
2. What are the company's IT policy priorities?
3. What are the "business jewels" of the company (information, internal processes, client databases, reputation, brand name, etc.)?
4. What is the impact if one of these "jewels" disappears or is badly compromised?
5. What kind of plan can be used to protect the company's business continuity against all threats?
6. How many times a year could this plan be tested?
7. How quickly could this plan be updated following company business changes?

The standard Risk Management and Risk Assessment Methodology (ISO 17799), which is almost certainly too comprehensive for SMBs, can help in responding to this question list. As an alternative, readers might care to visit <http://www.17799.com/> and ENISA's Web site for risk management comparison [http://www.enisa.europa.eu/rmra/rm\\_home.html](http://www.enisa.europa.eu/rmra/rm_home.html)

One last, but critical, point is that at every stage of this process, SMBs should consider the added value of what they propose.

---

## **Copyright Notice**

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

For further information regarding this document please contact:

Marketing Department

Tel: +44 (0) 20 8987 7100

Copyright 2006 IDC. Reproduction without written permission is completely forbidden.