



Efficiently Securing Your Business Through IT Security Outsourcing: A Call to Action for SMBs

Executive Summary

Small and medium businesses (SMBs) need to focus on a number of key business challenges: reducing costs, improving employee productivity and building competitive advantage. But a wave of new IT security attacks on SMBs, mounted by a new class of professional criminal hackers, is taking a heavy toll on SMBs, hurting profitability and growth goals.

Most SMBs are struggling ineffectually against this onslaught, and they don't have the attention, resources or technical skills in-house to do the job. Consequently, SMBs deal with IT security issues only intermittently, often in crisis-response mode, exposing themselves to unacceptably high risks.

Yankee Group believes that specialty IT security outsourcers can do a better, more cost-effective job of managing IT security than most SMBs. SMBs should seriously consider the benefits of outsourcing such functions as antivirus, personal firewalls, antispam and antispyware, and look for providers that can provide a reputable brand, the right suite of services, financial viability, a strong support organization and a road map to address emerging IT security threats.

“In general, we outsource things that have one of three characteristics: they’re complex, important or distasteful. Computer security is all three. Its distastefulness comes from the difficulty, the drudgery and the 3 a.m. alarms. Its complexity comes out of the intricacies of modern networks, the rate at which threats change and attacks improve, and ever-evolving network services. Its importance comes from this fact of today’s business world: Companies have no choice but to open their networks to the internet.”

**- Bruce Schneier, Founder, Counterpane
Internet Security**

Table of Contents

I. SMB Owners Focus on Running Their Businesses, Not Information Technology	2
II. SMBs Are now Targeted by Professional IT Criminals	3
III. SMBs Face an IT Security Threat Gap: You're Only as Good as Your Last Update	3
IV. SMBs Can't Afford Skilled IT Security Staff, Policies and Best Practices	4
V. The Case for IT Security Outsourcing	4
VI. Key IT Security Functions to Consider for Outsourcing.	5
VII. Recommendations: How to Evaluate IT Security Outsourcers	6
VIII. Glossary	6

I. SMB Owners Focus on Running Their Businesses, Not Information Technology

SMBs (which Yankee Group defines as organizations of fewer than 250 employees) are the great engines of modern economies. According to the U.S. Small Business Administration, SMBs comprise 95% of all U.S. businesses; generate more than half of the nation's gross domestic product; represent 26% of America's exporters; create 80% of all new jobs in the United States; and employ 52% of the private sector workforce. Yet the business environment for SMBs is more challenging than ever.

According to the Yankee Group *2004 SMB Infrastructure Survey* of SMB decision-makers:

- *Improving employee efficiency* is a major challenge for 33% of respondents.
- More than 25% cite *succeeding in an environment where the margin of error is low* as a major challenge.
- More than 80% now have mobile workers, a segment that engenders significant investments in productivity tools and serious cost management challenges.

- Most respondents are becoming increasingly reliant on e-mail and internet connectivity to communicate more quickly and responsively with partners, employees and customers. The majority of SMBs rate these technologies as more business-critical than the telephone; 38% cut shipping costs by sending documents electronically, and 52% reduced long-distance phone charges by interacting online or via e-mail. Most expect this reliance to increase as they consider new initiatives, such as internet telephony services based on VoIP technology.

Despite a growing reliance on information technology, SMB managers remain focused on a few key issues: reducing their capital and operating expenses; improving employee productivity and satisfaction; and improving or extending their competitive advantage. These challenges are daunting enough to occupy the vast majority of an SMB owner's attention. Most executives view IT as a critical means to achieving these goals, yet virtually none have the time, resources or technological expertise to continually evaluate and deploy improvements to their increasingly important IT infrastructure.

II. SMBs Are now Targeted by Professional IT Criminals

Unfortunately for SMB owners, the IT infrastructure which they already lack adequate resources to manage has rapidly become the target of a new class of professional hackers, criminals whose goals are to steal intellectual property, competitive information, sensitive customer and employee data, and financial information.

Not long ago, the most likely threat an SMB might face on the technology front was the defacing of the company web site by computer-adept teenager, the equivalent of graffiti sprayed on the walls of the headquarters facility. Such attacks might be embarrassing and entail some cost to clean up, but had little lasting impact.

By the year 2004, the majority of IT security attacks were being conducted by a new breed of hacker motivated by economic gain, running schemes ranging from identify theft and online fraud to corporate blackmail, espionage and extortion. These professionals draw from highly skilled software, network and security engineers around the globe, armed with a freely available arsenal of hacking tools, efficiently and anonymously forming ad-hoc criminal gangs over the internet.

SMBs are now under assault on a variety of fronts. Spammers clog e-mail inboxes with unwanted messages, gobbling IT resources such as bandwidth, server processing power and storage, and wasting employees' time sifting through the junk mail to get to the legitimate e-mails they need to do their jobs. Viruses and worms wreak havoc by destroying or stealing sensitive and valuable data and bringing employee productivity to a halt by crashing PCs, servers and networks. New threats like spyware insidiously infest users' machines, sapping PC performance while stealing information about employees' web usage, and robbing web advertisers of revenue via browser redirection or superimposed competitors' ads.

III. SMBs Face an IT Security Threat Gap: You're Only as Good as Your Last Update

SMBs have been fighting this new breed of assailants with some familiar technology weapons, such as network firewalls, desktop firewall and antivirus software, and antispyware and antivirus engines for e-mail servers. New threats like spyware will require new defenses, like antispyware and intrusion prevention software for the desktop. These countermeasures must be deployed, managed and continually updated as new threats are found. Antivirus and antispyware programs required continuous, incremental updates of signature files for new viruses and spyware agents. Desktop firewall software must be updated frequently to protect against new threats, and firewall rules changed to accommodate new applications.

The time between the availability of an update to a security mechanism and the actual deployment of that mechanism represents the so-called "threat gap"—the period in which the desktop, server, network or other critical resource is at risk of exposure to a new attack. In short, the IT infrastructure is only as secure as the latest update to its security mechanisms.

SMBs also face a growing burden of patch management. Hackers discover new vulnerabilities in Microsoft's operating systems, browsers and packaged applications every day. The task of identifying, prioritizing and deploying the patches and hot fixes that Microsoft now makes available on a monthly basis (as well as patches to other desktop applications) adds to the breadth of the threat gap, and heightens the challenge of bridging it with frequent updates.

Few SMBs have the resources to successfully manage and minimize this threat gap. The increasing mobility of employees adds to the problem. The laptops of field-based or traveling workers may be inaccessible to IT personnel during periodic security updates. These employees will continue to be exposed to all the vulnerabilities that have emerged since their last update, placing them at risk of attacks on data privacy and productivity. Worse, the next time they connect to the company network, they may

expose the rest of the organization to any viruses and worms they have picked up while their machines were in the threat gap.

The economic consequences are staggering: a recent Computer Security Institute/FBI Computer Crime survey revealed that virus attacks resulted in losses of \$27 million among 530 survey respondents. This amounts to billions of dollars spent by SMBs dealing with malicious code.

Failure to maintain current defenses against spam is also extremely costly. Around 50% of all messages sent to the .com domain are spam, which translates to a measurable productivity cost. Consider: spending 10 seconds per day deleting spam adds up to 60 minutes per year (10 seconds x 365 days divided by 60 equals 60.83 minutes). This sounds benign, but a company with 100 e-mail users faces a productivity loss of \$2,750 a year (1 hour per employee x \$27.50 average hourly wage). Users also admit to reading unsolicited e-mail. Spending just 1 minute per week reading junk mail creates an additional \$2,200 loss of productivity in a 100-employee company (1 minute x 48 weeks x \$27.50 average hourly wage x 100 employees divided by 60).

IV. SMBs Can't Afford Skilled IT Security Staff, Policies and Best Practices

Most SMBs don't have dedicated IT security personnel to minimize the threat gap. Security expertise is among the most in-demand and expensive IT skills. IT security professionals need ongoing training and certification, attendance at one or two industry-specific conferences per year, and sophisticated diagnostic tools. Salaries for security engineers typically range from \$60,000 to \$100,000, while security managers' salaries can reach \$150,000 and higher. These figures are reflected in a recent Yankee Group survey, which found that 25% of IT spending (the single largest expense) is allocated to staffing costs.

Many SMB managers would like to emulate the IT security best practices of their peers in large enterprises. Ideally, the SMB owner would be able to invest in a multilayered IT security infrastructure defense and hire expensive staffers to

keep it running smoothly. This dedicated IT security staff would baseline the security posture of the IT infrastructure, monitor it continually over time, and produce periodic reports showing continuous improvements.

The company would develop an IT security policy manual outlining the best practices that every employee must follow to protect sensitive company data and ensure their own productivity. Employees would receive regular formal training on these policies and practices. The company would automate security updates as much as possible. All employees would receive 24/365 support for IT security issues, regardless of their location.

Obviously, such initiatives are a luxury far beyond the means of most SMBs. Yet the growing criminal sophistication of attacks on an increasingly critical IT infrastructure demands that SMB owners respond somehow. The adverse impact on SMB costs, employee productivity and competitiveness cannot be ignored—but it's clear that few SMBs are successfully dealing with the problem.

V. The Case for IT Security Outsourcing

The growth and impact of outsourcing has emerged as one of the most important business trends of the last 10 years. SMB owners struggling to close an IT security threat gap that is increasingly difficult to manage in-house should consider these classic signifiers of a business case for outsourcing:

- Is managing IT security currently a core competency of the business, and is it likely to become more or less of a critical competency during the next few years?
- Would off-loading IT security allow the company to redeploy staff to focus on other, more valuable activities?
- Does managing IT security in-house add to or detract from the company's profitability and growth in any way?
- Could outsourcing of IT security management be achieved at little or no incremental cost, but with some measurable improvement in quality?
- Are the secondary costs of managing IT security (e.g., staffing costs) growing or shrinking?

The primary argument for outsourcing is financial: A company can outsource the security expertise it needs much more cheaply than hiring its own internal staff. Most companies would require several full-time, expensive, hard-to-find, hard-to-retain IT security employees, plus managers and backups, just to provide 24/365 IT security support. Industry estimates of cost savings of 20% and 60% through IT security outsourcing are common.

Outsourcing seeks to deliver these savings through several mechanisms. An IT security outsourcer brings economies of scale, employee leverage across customers, and career paths and salaries for security staffers that no SMB can hope to match. By spreading costs across many customers, IT security outsourcers can more cost-effectively hire security personnel with a broad range of competencies, build an infrastructure to support them, and keep them trained on new vulnerabilities, hacker tools, security products and software releases. IT security outsourcers also tend to have a much broader view of the IT security space, because they must respond to more varied customer problems on a daily basis. They can leverage knowledge gained from attacks against one customer for use in protecting all their customers.

VI. Key IT Security Functions to Consider for Outsourcing

SMBs managers who have concluded that outsourcing may make sense should consider the following commonly outsourced IT security functions:

- **Desktop and server antivirus:** Enables the initial deployment of antivirus software on every workstation and desktop, and optionally on (or in front of) application servers like e-mail servers. More important, the outsourcer provides automated, regular updating of antivirus signature files and periodic updates to antivirus software.
- **Desktop firewalls:** Enables the initial deployment of desktop firewall software on every workstation and desktop, and performs automated, regular updates to desktop firewall rules (according to security policies controlled by the SMB) and periodic updates to desktop firewall software.

- **Secure e-mail:** Installs, manages and maintains secure e-mail servers on behalf of the SMB. Optional security services typically include antispam services (with regular updates), server antivirus to screen out viruses before they reach users' inboxes (with regular signature updates), and content filtering services to protect employees from offensive or potentially fraudulent e-mails.
- **Antispyware and host intrusion prevention:** Enables the initial deployment of antispyware or host intrusion prevention software on every workstation and desktop, and regular updates to identify the behavioral signatures of new malware threats. These products scan for, root out and protect against the emerging and fast-growing threat of spyware and other malware agents—which can be downloaded through routine activities like web browsing; take root in desktops in ways which are difficult to detect and safely dislodge; and often evade signature-based threat detection systems like antivirus software.
- **Endpoint security policy enforcement:** Provides a health check of all remote PCs attempting to connect to the company via dialup, remote access VPN connectivity, wireless LAN access, direct connection to the corporate LAN, etc. Predefined security policies define what constitutes a healthy endpoint: patches and hot fixes installed, antivirus running with up-to-date signature files, personal firewall software running with the appropriate rules base, etc.

PCs that pass the health check, validated during the connection attempt with the help of a preinstalled agent or an external vulnerability scan, can connect to the network as usual. Unhealthy PCs are denied access or allowed to connect only to a quarantine subset of the network, until they take appropriate remediation steps (e.g., updating antivirus signature files). This important emerging security measure helps prevent infected PCs from spreading malware to other company systems.

VII. Recommendations: How to Evaluate IT Security Outsourcers

Yankee Group believes the majority of SMBs will outsource some of their IT security functions within the next 5 years and will outsource almost 90% of IT security functions within 10 years. The real intellectual property for security resides in advanced algorithms, intelligence and the ability to rapidly deploy new security countermeasures in real time. In other words, the value of IT security lies in the service, not the underlying infrastructure. SMB managers should focus on the following characteristics when shopping for IT security outsourcers:

- **Market presence and acceptance:** Choose a provider with a known and respected brand, and significant uptake as represented by market share leadership. IT security is too important to entrust to an unproven upstart.
- **Viability:** Make sure the provider has the financial resources and stability to survive the length of your contract. No one enjoys scrambling to find an alternate supplier when a primary service provider goes out of business unexpectedly.
- **Breadth of relevant services:** Recognize that no IT security outsourcer can be every thing to every customer. Choose a provider that can deliver the mix of IT security functions you want to outsource.
- **Quality and footprint of service organization:** Make sure the provider has a help desk and field support staff that you can reach 24/365, and that can physically get to your locations within an acceptable response window. Choose a provider with a strong local presales technical support team; this is often a leading indicator of long-term satisfaction with the service.
- **Cost and return on investment (ROI):** Shop around for the best price among the two or three leading candidates; this is one of the key drivers of any decision to outsource. But be wary of choosing a low-cost provider that doesn't meet the foregoing criteria. Unlike large enterprises, for which the complexity of security outsourcing increases the time to realize cost savings, SMBs should expect a quick ROI, certainly no more than 2 years. Ask for an upfront analysis that demonstrates your anticipated time to recover your investment.

- **Vision:** Get a clear understanding of how and when your provider intends to cover existing gaps in its service offering. If necessary, under the cover of a nondisclosure agreement, obtain an estimated timeline for the availability of antispymware functionality, endpoint security policy enforcement, network-based intrusion prevention services, VoIP security and other countermeasures for emerging threats. New vulnerabilities and exploits are a certainty; IT security vendors will always need time to catch up and integrate new features with existing services. Get a road map of your provider's near-term future enhancements.

VIII. Glossary

- **Antispymware:** Software that runs on desktops, servers or network security devices to detect, remove and prevent further installations of spyware.
- **Antivirus:** Software that runs on desktops, servers or network security devices to detect, remove and prevent further installations of viruses.
- **Content filtering:** Software or hardware, often residing in a network security device, that blocks or filters inappropriate, undesirable or dangerous internet content.
- **Firewall:** Software or hardware that filters network traffic to block unauthorized outside access to a protected network, while giving the protected network access to external networks. Network firewalls are typically deployed between private networks and the public internet. Desktop firewalls filter all network traffic in and out of a workstation or laptop.
- **Hacker:** Formerly a slang term for a computer enthusiast with little formal training. Increasingly, a synonym for "cracker," an unethical or criminal hacker who attempts to gain unauthorized access to computer systems and networks for the purpose of stealing or corrupting data.
- **Hot fix:** Software that fixes a bug in an application, utility or operating system, often combined in a group of fixes known as a service pack.

- **Intrusion prevention:** Software or hardware designed to detect and mitigate attacks on the security of a network or computing platform. Network-based intrusion detection systems usually take the form of security appliances, while host-based intrusion detection systems are installed as software on servers and desktops.
- **Malware (malicious software):** A generic term for any program that is harmful to a computer user, including viruses, worms, Trojan horses and spyware.
- **Patch:** A software repair for a bug in a computer operating system, utility or application, usually developed and distributed as a replacement for or an insertion in compiled software.
- **Patch management:** The process of acquiring, testing and installing multiple patches (code changes) to a set of computer systems. Specialized patch management systems help IT administrators track available patches, determine where and when to install them, validate their successful installation, and document patching policies and procedures.
- **SMB (small and medium business):** A business organization of fewer than 250 employees.
- **Spam:** Unsolicited bulk e-mail originating on the internet, the high-tech equivalent of unsolicited telephone marketing calls. Spam is an increasingly costly nuisance that drains computing, storage, network and end-user productivity resources.
- **Spyware:** Software residing on a user's desktop that aids in gathering information about a person or organization without their knowledge. It usually installs itself as part of the installation of free software, via web browsing, or through active computer viruses. Its distinguishing characteristic from other types of malware is that it seeks to evade detection so that it can continue collection information about the system on which it resides. Spyware is increasingly used by criminals to steal sensitive information, as well as a growing burden on IT help desks responding to users whose PC performance suffers because of extensive spyware infestations.
- **Threat gap:** A Yankee Group term that identifies the time between the availability of an update to a security mechanism and the actual deployment of that mechanism (e.g., the time that a patch or hot fix has become available from a software vendor, and the time that an organization actually installs it on its servers and workstations). Companies are vulnerable to external attacks during this period.
- **Trojan horse (or simply Trojan):** Malware hidden in otherwise harmless or useful applications or data.
- **Virus:** A program that replicates by being copied or copying itself to another program, computer boot sector or document. Viruses can be transmitted as attachments to an e-mail, in a downloaded file, or in removable storage media such as a CD, usually without the originator's knowledge. Some viruses deliver their payload as soon as their code is executed; others are triggered at a later time. Viruses are increasingly harmful, used to steal sensitive data, log user keystrokes, destroy files stored on hard drives, etc.
- **Worm:** A self-replicating virus that resides in active memory of a desktop or server. Unlike other virus types, worms propagate via vulnerabilities in operating systems, applications and networks without requiring action by an end user (e.g., opening an e-mail attachment, downloading freeware from a web site, copying a file from a portable USB drive) to propagate. Modern worms can propagate with frightening speed, wreaking costly havoc in the form of network, server and desktop downtime.

The Yankee Group

World Headquarters

31 St. James Avenue
BOSTON, MASSACHUSETTS 02116-4114
T 617.956.5000
F 617.956.5005
info@yankeegroup.com

Regional Headquarters

North America

31 St. James Avenue
BOSTON, MASSACHUSETTS 02116-4114
T 617.956.5000
F 617.956.5005
info@yankeegroup.com

951 Mariner's Island Boulevard, Suite 260
SAN MATEO, CALIFORNIA 94404-5023
T 650.522.3600
F 650.522.3666
info@yankeegroup.com

EMEA

55 Russell Square
LONDON WC1B 4HP
UNITED KINGDOM
T 44.20.7307.1050
F 44.20.7323.3747
euroinfo@yankeegroup.com

For More Information

T 617.956.5000
F 617.956.5005
E-mail: info@yankeegroup.com
Web site: www.yankeegroup.com

Advisory Services

Yankee Group advisory service annual memberships offer clients access to research and one-to-one expert guidance.

Advisory services represent our best value for clients. The services help our members understand industry, regulatory, competitive and market-demand influences, as well as opportunities and risks to their current strategies.

Membership includes an invaluable in-person strategy session with Yankee Group analysts, direct access to a team of analysts, research reports, forecasts, research notes and regular audioconferences on relevant topics.

We offer advisory services on almost 30 selected topics in Telecommunications; Wireless/Mobile Communications; Consumers, Media & Entertainment; and Information Technology Hardware, Software & Services.

Decision Instruments

Yankee Group offers a full portfolio of technology and market forecasts, trackers, surveys, and total cost of ownership (TCO), return on investment (ROI), selection and migration tools. Decision instruments provide our clients the data required to compare, evaluate or justify strategic and tactical decisions—a hands-on perspective of yesterday, today and tomorrow—shaped and delivered through original research, in-depth market knowledge and the unparalleled insight of a Yankee Group analyst.

Trackers

Trackers enable accurate, up-to-date tactical comparison and strategic analysis of industry-specific metrics. This detailed and highly segmented tool provides discrete proprietary and performance data, as well as blended metrics interpreted and normalized by Yankee Group analysts.

Surveys

Surveys take the pulse of current attitudes, preferences and practices across the marketplace, including supply, delivery and demand. These powerful tools enable clients to understand their target customers, technology demand and shifting market dynamics.

Forecasts

Forecasts provide a basis for sound business planning. These market indicators are a distillation of continuing Yankee Group research, interpreted by our analysts and delivered from the pragmatic stance our clients have trusted for decades.

Signature Events

Yankee Group's signature events provide a real-time opportunity to connect with the technologies, companies and visionaries that are transforming Telecommunications; Wireless/Mobile Communications; Consumers, Media & Entertainment; and Information Technology Hardware, Software & Services.

Our exclusive interactive forums are the ideal setting for Yankee Group analysts and other industry leaders to discuss and define the future of conversable technologies, business models and strategies.

Consulting Services

Yankee Group's integrated model blends quantitative research, qualitative analysis and consulting. This approach maximizes the value of our solution and the return on our clients' consulting investment.

Each consulting project defines and follows research objectives, methodology, desired deliverables and project schedule. Many Yankee Group clients combine advisory service memberships with a custom-consulting project, enabling them to augment our ongoing research with proprietary studies.

Thousands of clients across the globe have engaged Yankee Group for consulting services in order to hone their corporate strategies and maximize overall return.

www.yankeegroup.com

Yankee Group believes the statements contained in this publication are based on accurate and reliable information. However, because our information is provided from various sources, including third parties, we cannot warrant that this publication is complete and error-free. Yankee Group disclaims all implied warranties, including, without limitation, warranties of merchantability or fitness for a particular purpose. Yankee Group shall have no liability for any direct, incidental, special, or consequential damages or lost profits. This publication was prepared by Yankee Group for use by our clients.