

Five Ways in—Securing your Business in Tough Economic Times

The big picture for small and medium-size businesses

The Harsh Realities

The world economy is “entering a major downturn”—According to the International Monetary Fund’s (IMF) most recent World Economic Outlook, rich-country financial markets are experiencing “the most dangerous shock” since the 1930s

The global unemployment rate will rise to 6.1 percent in 2009—The IMF forecasts an increase in the number of unemployed by 18 million people in 2009 in comparison to 2007 when the global unemployment rate was at 5.7 percent

Gross domestic products (GDP) for Germany, France, and Italy are shrinking—According to the IMF, the U.K. has seen worst performance of any major economy in 2008

The U.S. unemployment rate rose to 7.6 percent in January 2009—This surpassed 1993 figures. In the past 12 months, the number of unemployed persons has increased by 4.1 million. [Source: Bureau of Labor Statistics]

The world economy is on shaky ground, and anxiety is running high in all business sectors. Virtually all global markets are being affected by the grim economic reality. And, in a downturn of this magnitude, the specter of cybercrime looms larger than ever before. Just as the 2001 to 2002 recession in the U.S. was accompanied by an increase in cybercrime, the pattern is repeating today all over the world. As McAfee® Avert® Labs suggests, “Recession is fertile ground for criminal activity as fraudsters clamor to capitalize on the rising use of the Internet and the climate of fear and anxiety.” Despite dwindling budgets and IT resources, businesses of all sizes need to take a good, hard look at how well their investment in digital security will help them stay a step ahead of opportunistic organized cybercriminals motivated by profit—and even laid-off, disgruntled employees who turn to data theft as a way out of their financial rut.

Small and medium-size businesses (SMBs) are particularly vulnerable because they are strapped for time and resources. In this series of five articles, we take a look at how McAfee empowers SMBs with Smart. Simple. Secure. solutions to see them through tumultuous times and lay the foundation for stronger security for the future.

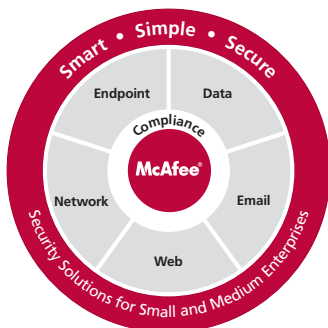
What is *Smart. Simple. Secure.*?

- *Smart*—Consolidation of security solutions with built-in intelligence in a single solution
- *Simple*—Easy to deploy, easy to view, and easy to administer from a single management console
- *Secure*—Uncompromising IT security and support from the world’s largest dedicated security company

Cybercrime flourishes amid economic uncertainty

As the economy weakens, cybercriminals are becoming more industrious, more pervasive, and more sophisticated. Advanced Internet technologies like Web 2.0 offer greater interactivity and richer content for users, but they also open the door to socially engineered threats on popular websites such as Facebook and YouTube. Cybercriminals are increasingly using automation to fool more of the people more of the time. According to the *McAfee Cybercrime versus Cyberlaw: 2009 Virtual Criminology Report*, the number of zombie PCs used in botnets has quadrupled in the last quarter alone—and these botnets are capable of flooding the Internet with more than 100 billion spam messages per day.

Over the span of a year—from the end of 2007 when the economy started to slide—to the end of 2008, the percentage of malware of all varieties has escalated dramatically.



McAfee Avert Labs Threat Statistics	End of 2007	End of 2008	Percentage Growth
Password stealers (main variants)	80,000	380,000	375%
Malware (main variants)	586,000	2,700,000	361%
Malware (collection)	5,800,000	16,300,000	181%
Malware families (.DAT-related)	358,000	484,000	35%
Vulnerabilities	28,500	34,100	20%
Potentially unwanted programs	24,000	26,000	8%

Examples of recent threats:

- According to McAfee TrustedSource, 82 percent of all email is spam
- “Online theft costs one trillion a year, the number of attacks is rising sharply, and too many people do not know how to protect themselves,” announced a panel of security experts at the World Economic Forum [Source: *BBC News Online/Interactive*]
- Earlier this year, hackers broke into the Federal Aviation Administration’s computer system, stealing 45,000 names and Social Security numbers of employees and retirees. [Source: *NetworkWorld*]
- Since November, 2008, the Conficker worm has infected more than 10 million PCs. The trick behind this exploit is to disable anti-malware protection and block access to websites of anti-malware vendors. It’s so insidious and widespread that Microsoft is offering a \$250,000 reward to bring the Conficker bad guys to justice. [Source: *NetworkWorld*]

The threat landscape is getting worse by the day, and the global recession is adding fuel to the fire. Avert Labs cites that in 2008, more than two million unique pieces of malware were identified, more than all the malware in the preceding five years combined. Even websites that appear to be safe are not immune from compromise. In an uneasy economic climate, employees are more easily duped and distracted as cybercriminals take advantage of victims by developing socially engineered threats based on trends and tendencies related to the financial crisis. Networking sites like LinkedIn, which professionals rely on to stay in touch with business contacts and seek employment opportunities, are being leveraged by cyber crooks to lure visitors to malicious sites that steal identities, credit card information, or infect PCs with malware.

Aside from crimes perpetrated by organized hacker rings, data theft by employees is also on the rise. Facing possible workforce reductions, some employees are misappropriating corporate assets for their own financial gain. Employees seeking better opportunities are pilfering valuable intellectual property and turning over the goods to competitors that reward them with higher salaries or bonuses. Others are stealing confidential customer information and building databases to lay the groundwork for their own businesses. And distracted or untrained employees can put a business at risk by intentionally leaking sensitive data, losing a company laptop or mobile phone that stores sensitive information, or falling victim to a cyber threat—even in the best of times.

The far-reaching business impact of cybercrime

Undoing the damage of cybercrime can be an expensive proposition. Dealing with a threat can cost a lot of money in overtime pay for IT staff working late hours to fix the problem or in fees for external contractors. Once a system is infected with a Trojan or a rootkit, it can cost a business hundreds of dollars per system to clean it. Loss of productivity also adds to the cost. Imagine if 500 users could not use their systems for three hours while maintenance and patching is performed—that adds up to 1,500 paid man-hours of work with absolutely no return.

A weak economy calls for even stronger security: SMBs gear up

The good news is that SMBs are taking cyber threats seriously and are starting to invest in security. A Gartner Research report, *User Survey Analysis: IT Spending Plans in the SMB Market, North America, 2008*, predicted increases in spending. The report suggests that midsize businesses will increase IT spending by 5.34 percent over the year before. In spite of a sluggish economy, SMBs are recognizing the seriousness of cybercrime and are seeing the need to increase IT security budgets. Forrester's report, *The State of SMB Security: 2008-2009*, predicts that security spending for SMBs will increase by more than 10 percent—up from an approximately nine percent increase in 2008.

Small and medium-size businesses have five top priorities when it comes to protecting their business information and infrastructure from economically motivated attacks: endpoints, data, email, web, and the network.

- *Endpoints*—Desktops, laptops, and servers are vulnerable to distributed denial-of-service (DDOS) attacks, viruses, rootkits, Trojans, web-based spyware, phishing scams, and other exploits
- *Data*—Loss and leakage of vital information occurs through carelessness, theft, or unauthorized access. Hackers get their hands on valuable corporate information through insecure access points, and unethical employees can easily transfer unprotected confidential data from laptops to USB drives.
- *Web*—Network perimeter vulnerabilities can open the door to data breaches and also expose users to spyware, annoying adware popups, and phishing attempts. According White Hat Security, nine out of 10 websites are vulnerable to attack.
- *Email*—The spam that finds its way into employee inboxes isn't a mere nuisance any more. It has evolved into a serious threat that is often linked to attacks. Spam not only clogs mail servers and wastes valuable IT resources, it also puts company data and employees at risk.
- *Network traffic*—Systems that aren't well guarded are vulnerable to intrusions and malware from both internal and external threats. Network gateway systems are also the key to keeping communications secure while managing traffic between home or branch offices.

The best defense: following industry best practices

With threats becoming more numerous and more sophisticated, SMBs require proactive defenses that work together seamlessly. Consolidated protection with centralized management is critical for reacting quickly to outbreaks and to gain visibility into compliance status. Natalie Lambert, in Forrester's 2008 *Client Security Report*, states "... consolidated solutions will offer the desktop operations team everything they need to manage the PC life cycle as well as the resident data."

Consolidation and integration of point products not only provides smarter protection, it also lowers costs. Analysts like Forrester and Gartner Research recommend that SMBs follow these industry best practices:

- *Consolidate*—Stronger security can be achieved by consolidating security vendors and purchasing protection in suites rather than standalone products
- *Centralize management*—With a single management console at the hub, SMBs get greater visibility and increased control
- *Reduce costs*—Integrated solutions are more economical, resulting in savings in product costs and more efficient management and technical support

Smart. Simple. Secure.

McAfee offers an affordable single-vendor approach to SMB security—McAfee Total Protection for Secure Business. It's the *Smart. Simple. Secure* way to respond to the growing threat of cybercrime in today's economic climate.

Smart.

A major advantage of this approach for SMBs is integrated protection that extends to all five threat vectors—endpoints, data, email, web, and the network. Consolidated security and management eliminate the compatibility and maintenance issues associated with multiple point products and vendors and provide better visibility, control, and comprehensive intelligence on a business's security posture.

An integrated solution significantly reduces costs—by as much as 50 percent on licensing and support compared to a point-product approach. With a unified solution and technical support, SMBs can make more informed decisions about handling attacks when they strike and can anticipate new threats. And auto-updating gives them the confidence that their protection is always current, so they stay steps ahead of cyber crooks.

Simple.

With centralized management at the hub, McAfee security solutions for SMBs are easy to deploy and maintain. Rather than burdening an already busy IT staff with learning and managing multiple consoles for point products, SMBs can deploy McAfee ePolicy Orchestrator® (McAfee ePO™) to simplify monitoring, maintenance, and reporting. Research conducted by Insight Express for McAfee shows that customers using ePO expend 75 percent less time and effort to manage their security than customers who use other management systems. By using ePO effectively and by following some fundamental practices recommended by McAfee, busy IT professionals can spend as little as 15 minutes per day proactively managing security. McAfee shows SMBs how they can prioritize activities and stay on top of their security with daily, weekly, and monthly actions, including checks and balances.

Secure.

With all “five ways in” covered by McAfee Total Protection for Secure Business, small and medium businesses benefit from stronger security to help them weather the storm today and safeguard their future. It provides all of the critical elements of security that SMBs require to combat cybercrime—anti-virus, anti-spyware, desktop firewall, host intrusion prevention, full-disk data encryption, device control, and three layers of web security, including URL filtering, malware scanning, and McAfee SiteAdvisor® to warn users about risky websites. SMBs can be assured that their protection is proactive and always up to date, thanks to threat intelligence gathered by McAfee Artemis Technology, which quarantines or blocks new threats even before a signature is developed—anytime, anywhere—reducing the protection gap to milliseconds.

Steps you can take to protect your business

There’s no time to waste when it comes to security—during tough economic times—or any time. Here are some things SMBs can do immediately to set their security plan in motion:

- Learn how to secure your business in just 15 minutes per day—the McAfee way
- Learn more about McAfee’s integrated security solutions for SMBs
- Educate yourself about the five key threat vectors and how to fortify your security by reading the articles in our series, *Five Ways In: Securing Your Business in Tough Economic Times*

