REAL WORLD CASE 1

F-Secure, Microsoft, GM, and Verizon: The Business Challenge of Computer Viruses

Mikko Hypponen and his band of Finnish computer virus hunters know the odds are stacked against them in the Web's wild frontier. "Tracking down a virus is rare," says Vincent Gullotto of the antivirus research lab at software maker Network Associates. So you'll have to pardon Hypponen, the antivirus research manager at Helsinki-based software company F-Secure Corp. (www.fsecure.com), if he got a little excited when he and his team were able to crack the SoBig virus before it finished doing whatever it was meant to do. Thanks to research from F-Secure, a 300-employee company known for cracking tough computer problems, virus experts and government investigators in several countries were able to shut down a network of computers hijacked by the virus just minutes before SoBig was to launch what was expected to be the next phase of its attack, "It was a very close call," says Hypponen. "The virus writers will make sure it's not as easy next time."

Indeed, to those most affected, it seemed as if the onslaught of viruses had reached epidemic proportions in August 2003, as the world's computer systems were blitzed by hundreds of viruses. On August 11, the Blaster virus and related bugs struck, hammering dozens of corporations, including Air Canada's reservation and airport check-in systems. Ten days later, the SoBig virus took over, causing delays in freight traffic at rail giant CSX Corp. and shutting down more than 3,000 computers belonging to the city of Fort Worth. Worldwide, 15 percent of large companies and 30 percent of small companies were affected by SoBig, according to virus software tracker TruSecure Corp. Market researcher Computer Economics Inc. estimates damage will total $2 billion—one of the costliest viruses ever. All told, damage from viruses may amount to more than $13 billion in one year.

Even as the damage reports pour in, the summer of SoBig provides a jangling wake-up call to businesses, consumers, and the software industry: Get serious about cybersecurity. At the same time, technology experts are warning of the dangers of relying so heavily on just one outfit—Microsoft Corp. (www.microsoft.com)—to provide the backbone of the computing and Internet world. With a 95 percent market share, Microsoft's Windows desktop operating system is a fat, juicy target for the bad guys.

Some critics even say that Microsoft, as a virtually essential service, has an obligation to ensure that its software is sufficiently hostile to hackers. Tech experts are calling on the company to make fundamental changes in the way it designs programs. "Microsoft has to write better software," says Paul Saffo, director of think tank Institute for the Future in Menlo Park, California. "It's outrageous that a company this profitable does such a lousy job."

Security experts and corporate tech purchasers say the glitches exist because Microsoft and other software companies have placed a high priority on getting products out quickly and loading them with features, rather than attending to security. They're calling on the industry—and Microsoft in particular—to make software more secure. Ralph Szygenda, chief information officer at General Motors Corp. (www.gm.com), got fed up when his computers were hit by the Nimda virus in late 2001. He called Microsoft executives. "I told them I'm going to move GM away from Windows," Szygenda recalls. "They started talking about security all of a sudden."

Amid much fanfare, Microsoft launched its Trustworthy Computing initiative in 2002, a campaign it claimed would put security at the core of its software design. As part of the campaign, more than 8,500 Microsoft engineers stopped developing Windows Server 2003 and conducted a security analysis of millions of lines of freshly written code. Microsoft ultimately spent $200 million on beefing up security in Windows Server 2003 alone. "It's a fundamental change in the way we write software," says Mike Nash, vice president for security business. "If there was some way we could spend more money or throw more people on it, believe me, we'd do it." Yet, embarrassingly, Windows Server 2003, released in April 2003, was one of the systems easily exploited by Blaster.

But the burden for combating viruses lies with computer users themselves. Most large corporations already have basic antivirus software. But security experts maintain that they need to come up with better procedures for frequently updating their computers with the latest security patches to programs and inoculations against new viruses. Verizon Communications (www.verizon.com) has gotten serious about security in the past couple of years and already has a system for automatically updating its 200,000 computers as soon as patches are available. As a result, it escaped unscathed from the summer attacks. "As far as business impact, it was a nonevent for us," says Chief Information Officer Shaygan Kheradpir.

Case Study Questions

1. What security measures should companies, business professionals, and consumers take to protect their systems from being damaged by computer worms and viruses?
2. What is the ethical responsibility of Microsoft in helping to prevent the spread of computer viruses? Have they met this responsibility? Why or why not?
3. What are several possible reasons why some companies (like GM) were seriously affected by computer viruses, while others (like Verizon) were not?

Source: Adapted from Steve Hamm, Jay Greene, Cliff Edwards and Jim Kerstetter, "Epidemic," *BusinessWeek*, September 2, 2003. Reprinted from 9/02/03 issue of *BusinessWeek* by special permission, copyright © 2003 by the McGraw-Hill Companies, Inc.