www.usatoday.com

USA TODAY

Money

SECTION B

Thursday, September 9, 2004

By Martin E. Klimek for USA TODAY

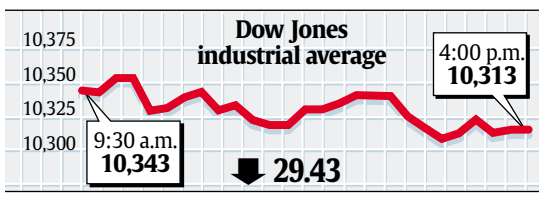
Attorney: Warrington Parker heads diversity efforts at law firm Heller Ehrman White & McAuliffe. "Race counts," he says.

Legal industry lacks color

'The statistics are shocking,' says author of report out soon. Fewer than 4% of firm partners are minorities. 3B

Moneyline

Wednesday markets



Index	Close		Change
Nasdaq composite	1850.64	▼	7.92
Standard & Poor's 500	1116.27	▼	5.03
Treasury bond, 30-year yield	4.96%	▼	0.05
Treasury note, 10-year yield	4.16%	▼	0.08
USA TODAY Internet 50	102.94	▼	0.05
e-Business 25	87.77	▼	0.08
e-Consumer 25	153.05	▲	0.06
Oil, light sweet crude, barrel	$42.77	▼	0.54
Euro (dollars per euro)	$1.2191	▲	0.0093
Yen per dollar	109.25	▼	0.14

Sources: USA TODAY research, MarketWatch.com

► Market scoreboard with currencies, 6B

Energy lowers prediction for heating costs

Winter heating bills for natural-gas users will rise 15% this season, not 20% as estimated a month ago, the Energy Department said Wednesday in a monthly report. More than half of U.S. homes use natural gas; last winter, their heating bills rose an average 8%. Energy expects heating bills to rise 6% for homes that use oil, not the 10% previously estimated. The lower predictions follow a mild summer that didn't sap supplies as much as expected. But oil prices are likely to remain above $40 a barrel, Energy said, so gasoline prices won't drop as much as usual this winter.

Viacom sets Blockbuster split-off ratio

Viacom kicked off its stock exchange with shareholders to split off its 82% stake in video rental unit Blockbuster. To entice investors to embrace the split-off, the owner of CBS, MTV and Paramount Pictures is offering a premium of 19% over Viacom class B shares. The deal values Viacom shares at $40.69, based on Blockbuster's Tuesday close of $7.90.

For Coke bottler, glass is half-empty

Shares of Coke's biggest bottler, Coca-Cola Enterprises, fell 5.4%, or $1.11, to $19.48 Wednesday after the company lowered its earnings outlook for the year and third quarter. The company expects annual earnings of $1.21 to $1.25 a share, rather than $1.48 and $1.52, because of soft sales in North America and Europe. The company expects third-quarter earnings of 38 to 40 cents a share. The news also hurt Coca-Cola stock, which fell 4.8%, or $2.20, to $43.45.

Apple's Jobs back on the job

Apple CEO Steve Jobs, who underwent pancreatic cancer surgery in late July, returned to work part time this week. Apple spokeswoman Katie Cotton says Jobs has attended some staff meetings and is expected to be back full time by the end of the month.

Consumer debt rises most since January

Consumers increased borrowing in July by the most since January, the Federal Reserve said Wednesday. Consumer credit increased at a seasonally adjusted annual rate of 6.4% in July after a 2.6% gain in June. Demand for revolving credit, such as credit cards, jumped 9%. Demand for non-revolving credit, such as loans for cars and tuition, rose 5%.

New menu items help McDonald's sales

New menu items helped lift McDonald's to a 16th-consecutive increase in monthly comparable-store U.S. sales, and the fast-food giant has more sandwiches on the way. The launch of Chicken Selects contributed to a better-than-expected 7.2% jump in August, McDonald's said Wednesday. The next offering might be Oven Selects, five toasted, delicatessen-style sandwiches being test-marketed at 400 McDonald's.

Telecom: More cellphone towers ahead

FCC appears set to ease rules. 3B

Tech: Can one handheld device do it all?

Personal Technology columnist Ed Baig test drives the new BlackBerry. 3B

► RealNetworks to continue offering downloads of some hit songs for 49 cents. 4B

Autos: Honda warns about CR-V fires

First oil, filter change must be done properly. 4B

Retailing: Wal-Mart CEO calls for change

Lee Scott says management must get out more to repair tarnished reputation. 5B

Media: Kerkorian close to MGM deal

Dueling bids from Time Warner, Sony, fall just under $5 billion. 5B

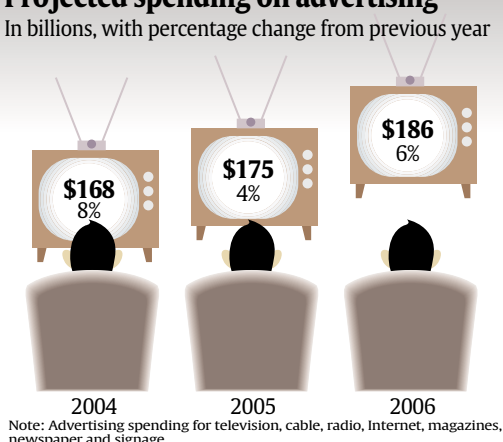
Compiled from staff and wire reports

Get business news and market data updated 24 hours a day, 7 days a week at money.usatoday.com

USA TODAY Snapshots

Projected spending on advertising

In billions, with percentage change from previous year



Note: Advertising spending for television, cable, radio, Internet, magazines, newspaper and signage
Sources: PricewaterhouseCoopers Global Entertainment and Media Outlook: 2004-2008

By Darryl Haralson and Alejandro Gonzalez, USA TODAY

Special report: PCs under attack — Part 2

Tech industry presents less-than-unified defense

It's up to individual owners to protect their computers

By Sam Ward, USA TODAY

By Byron Acohido and Jon Swartz
USA TODAY

Last fall, the Blaster Internet worm slammed into Cable Bahamas like a digital hurricane, clogging Web connections for the tiny Internet service provider's 22,000 subscribers.

"We got hammered," says Andre Foster, technology vice president for the Nassau-based company.

After recovering from Blaster, Foster began to rethink his main line of defense against Web attacks. Instead of relying on home PC users to lock down individual machines, he acquired costly hardware and software designed to screen out suspicious data coming into and out of Cable Bahamas' local system.

The result: Cable Bahamas' subscribers have gone largely untouched by the flurry of Web attacks this year. "Somebody has got to step up and at least attempt to protect the end user, and that's what we're trying to do," Foster says.

Comparatively few other tech suppliers are going as far as Cable Bahamas to help secure the Internet.

As cybercriminals toil with near-impunity, tech companies in the best position to make the Web safer — Microsoft, Internet service providers and anti-virus software makers — are failing to respond effectively to a snowballing threat, say security experts and industry executives.

Tech suppliers say they're doing all they can to make it easier for home users to secure their own PCs: guiding consumers to a raft of products and services they can use to lock out cyberintruders. But critics say that's akin to making car drivers responsible for installing their own seat belts.

"As long as we rely on the end user as the

Please see SPECIAL REPORT next page ►

How do hackers take over and use your PC?

See the graphic explainer at tech.usatoday.com

► Read the complete two-day report at tech.usatoday.com

Oil worries curb Fed chief's optimism

By Sue Kirchhoff
USA TODAY

WASHINGTON — Federal Reserve Chairman Alan Greenspan said Wednesday that the economy has "regained some traction" after a late spring slowdown caused largely by high oil prices.

In testimony economists called a clear signal the Fed plans to raise interest rates this month, Greenspan told the House Budget Committee that consumer spending and housing starts bounced back in July, business investment is on the upswing and the job market picked up in August. Despite high oil prices, inflation has eased in recent months.

The economy

But he added that retail sales have been mixed and cautioned that the outlook for oil prices "remains uncertain."

"The most recent data suggest that, on the whole, the expansion has regained some traction," Greenspan said, adding, "If it weren't for the oil price spike, I would be very optimistic about where the economy is going."

Economists expect the Fed to raise interest rates a quarter of a percentage point, to 1.75%, when policymakers meet Sept. 21. The central bank has already raised rates twice, from 1% in late June, to guard against a resurgence of inflation.

"The market has a (quarter-point) tightening priced in for Sept. 21. This was Greenspan's last chance to alter that expectation. He did not," says Steve Stanley of Greenwich Capital Markets.

By Pablo Martinez Monsivais, AP

Greenspan: Discusses economy Wednesday.

► Economy slowly expanding, 4B

Greenspan was more optimistic than some economists, who suggest the Fed could slow its rate campaign later this year if things don't pick up. For example, a recent rise in auto sales was spurred by dealer incentives, with companies now scaling back.

Greenspan said the recent slowdown in business activity, with the economy expanding at a 2.8% annual rate in the second quarter of 2004, "no doubt is related, in large measure, to this year's steep increase in energy prices." Oil prices soared near $50 a barrel this summer but have since fallen below $43.

The central bank chief tried to avoid being drawn into the political battle over the economy. Greenspan said President Bush's tax cuts had been well-timed, while acknowledging that other federal strategies could have been as effective.

But Greenspan took a tough line against budget deficits, forecast to top $400 billion this year. He asked Congress to reinstate and expand a law, in effect for much of the 1990s, requiring new programs or tax cuts to be paid for. Republicans, who control Congress, have resisted his pleas. He warned that high deficits could lead to rising interest rates, inflation and even "stagflation" — high inflation and low growth — as the baby boom generation ages, straining Medicare and Social Security. He called again for overhauling the programs.

Quattrone sentenced to surprising 1½ years in prison

By Thor Valdmanis
USA TODAY

NEW YORK — Frank Quattrone was sentenced to a harsher-than-expected 18 months in prison Wednesday after a federal judge ruled that the former star investment banker lied during testimony in his obstruction-of-justice trial.

The severity of the sentence stunned Quattrone's family and friends and sent a chill wind through Silicon Valley, where the popular 48-year-old is regarded as a scapegoat for the crimes of Wall Street during the boom years. A probation report had recommended five months in prison and five months' home detention for obstruction of justice — identical to Martha Stewart's sentence for a similar crime.

"The judge threw the book at Quattrone," said former prosecutor Jacob Zamansky, who attended much of the trial. "Stewart got a lenient judge and a lenient sentence. Quattrone got a tough judge and a tough sentence."

Federal Judge Richard Owen also rejected a joint prosecution-defense motion that Quattrone be allowed bail pending appeal.

"The people have spoken," Owen told a packed courtroom.

He ordered Quattrone to begin serving his sentence in 50 days, likely at the minimum-security Lompoc prison camp near Quattrone's Northern California home. Quattrone, who made up to $120 million a year taking high-tech companies public as a Credit Suisse First Boston banker, was also fined $90,000 and given two years' probation.

Reuters

Quattrone: Must report in 50 days.

Quattrone's crime was sending a 22-word e-mail to former CSFB colleagues on Dec. 5, 2000, encouraging them to "clean up" their files. In May, a jury convicted him on three counts of obstructing federal investigations into whether some CSFB clients had paid kickbacks to get shares in hot initial public offerings. Owen said Quattrone lied when he said he did not intend to obstruct the investigations.

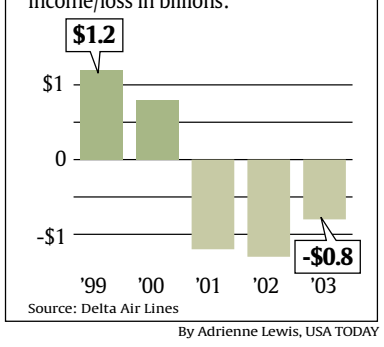
Outside court after the sentencing, Quattrone said, "To my family in California, I'm coming home soon. I'm OK, and I love you. I can hold my head high right now, because I know I'm innocent."

Quattrone's wife is chronically ill, and Quattrone's lawyers said his 15-year-old daughter has psychological problems. Owen said the impact on the family could be softened by its financial assets: Quattrone's wife has $50 million, and his daughter has $26 million in a trust fund.

Lawyers for Quattrone vowed to win on appeal, arguing Owen kept out critical evidence offered by the defense.

Delta's drop

For the first half of 2004, Delta had a net loss of $2.3 billion. Annual net income/loss in billions:



Source: Delta Air Lines

By Adrienne Lewis, USA TODAY

Delta's last gasp: Reduce staff 10%

By Dan Reed
USA TODAY

Delta Air Lines will cut its staff 10% in the next 18 months in a bid to survive the financial downturn that has seen $5.6 billion in losses since 2000.

In a Webcast on Wednesday, CEO Gerald Grinstein laid out for employees and the public, for the first time, extensive savings proposals that he said will result in "a new airline for (a) new environment."

Airlines

He warned that Delta will file for bankruptcy-court protection if its pilots don't agree soon to concessions valued at $1 billion a year. Delta's debt holders, creditors and suppliers also must agree to concessions "in the near term" to avert a bankruptcy filing, he said.

"The permanently changed aviation marketplace and Delta's unsustainable financial losses confirm that our survival requires a viable cost structure," Grinstein said.

► U.S. airlines in trouble, 5B

Delta's goal: Cut $5 billion in annual expenses by 2006, measured against 2002. By year's end, $2.3 billion in cuts will be in place, leaving $2.7 billion more to be cut.

The largest cut, $1 billion, must come from pilots, Grinstein said. The Air Line Pilots Association has offered concessions it values at $705 million.

Grinstein also warned that Atlanta-based Delta could be forced into bankruptcy court if a deal slowing the rate of pilot retirements isn't reached by month's end. He said Delta might not be able to staff all its flights.

But Chris Renkel, ALPA spokesman at Delta, said the union has already agreed to changes to keep Delta's flights fully staffed.

The No. 3 U.S. airline's makeover plans call for eliminating as many as 7,000 jobs and cutting pay and benefits of remaining workers. A new employee reward program, including profit sharing, performance-based incentives and stock, could offset those cuts. Other plans:

► Closing its Dallas/Fort Worth hub, a chronic money loser, by February. Delta will slash daily flights at DFW airport to 21 from 254.

► Expanding remaining hubs at Atlanta, Cincinnati and Salt Lake City.

► "De-peaking" its Atlanta hub, spreading arrivals and departures evenly throughout the day.

► Expanding Song, Delta's lower-cost brand, initially by adding 12 planes to its fleet of 36.

► Retiring four of its 11 aircraft types by 2008.

Airline consultant Ron Kuhlmann at Unisys R2A praised Grinstein for laying out the "clearest delineation of a path forward" of any big airline.

Analyst Dan McKenzie at Smith Barney said problems remain. Bondholders seem reluctant to modify debt terms, and pilot retirements are draining badly needed cash, he said.

Special report: PCs under attack – Part 2

Rivalries, cost fears hinder cooperation

Continued from 1B

primary mechanism to secure their own computer, we will continue to have large quantities of unsecured devices," says Mitchell Ashley, chief technology officer at StillSecure.

In the past eight months, USA TODAY interviewed more than 100 tech industry executives, consultants, analysts, regulators and security experts who say tech suppliers could be doing much more to buttress Internet security. In pointing fingers, critics say that Microsoft could do more to supply basic protection for every Windows PC, that Internet service providers could significantly tighten key Web gateways, and that anti-virus companies could move more quickly to develop and distribute smarter software.

Instead, leading tech suppliers — bedeviled by competitive rivalries and hesitant to bear more product-support expenses — have proved incapable of joining forces to put up a unified defense, which is what it will take to clean up the Web, critics say.

"They're not working together, and because they're not working together, they're putting all of us at risk," says Alan Paller, research director of SANS Institute, a Washington-based Internet-security think tank and training center.

Much is at stake. Worldwide losses from cyberattacks will swell to an estimated $16.7 billion by the close of the year, up from $3.3 billion in 1997, according to tech consultant Computer Economics. As cyberattacks become more invasive, businesses across the USA are becoming wary of using e-mail as a tool. Some are pulling back plans to open more of their networks to customers, partners and mobile workers.

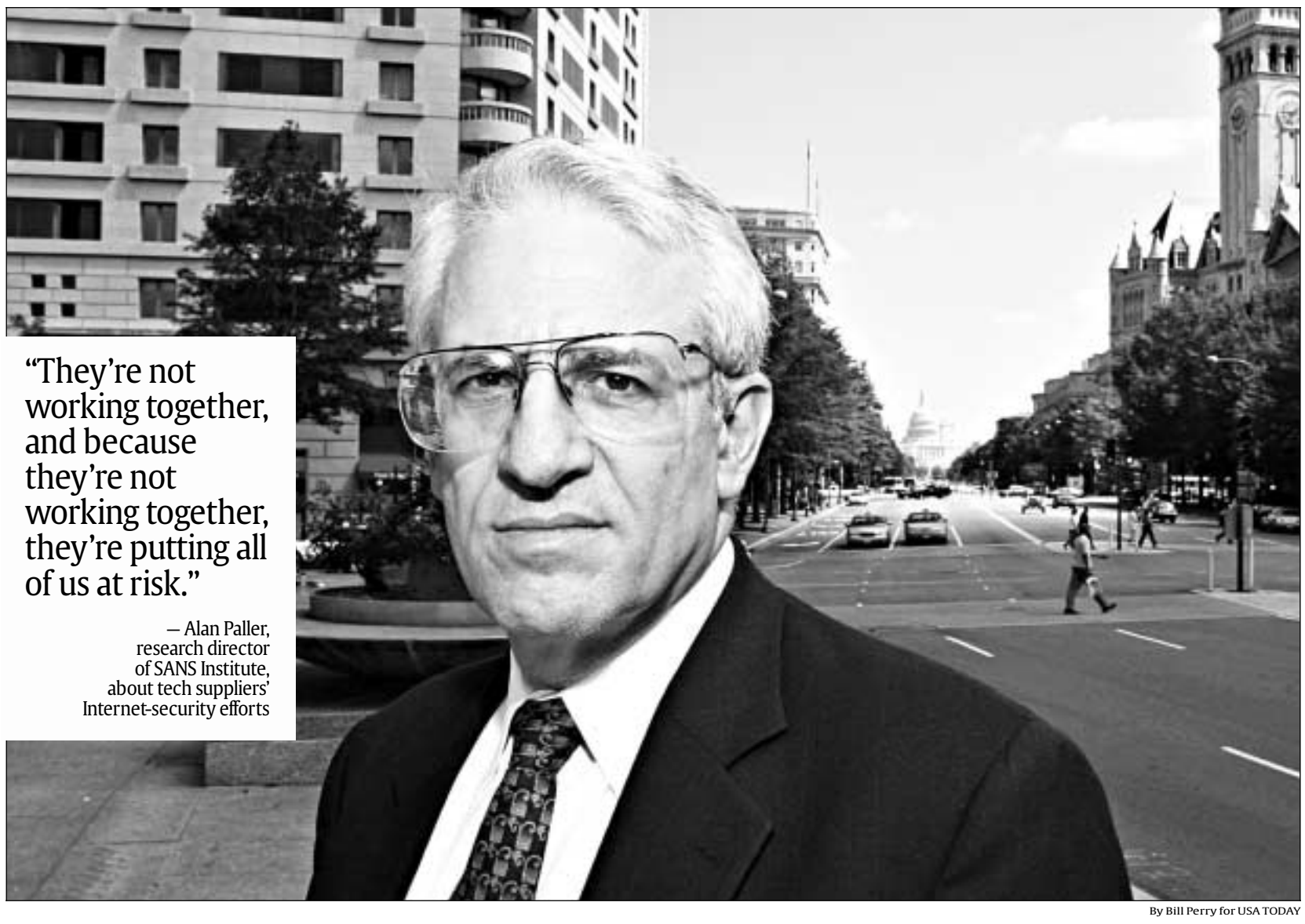
Meanwhile, consumers remain largely ignorant about the extent of the threat. Cyberintruders have begun to wrest control of millions of PCs in homes, small businesses, college campuses and government agencies. Compromised PCs are being transformed into obedient zombies slotted into underground networks to broadcast spam, carry out identity theft scams, even conduct cyberblackmail.

What's needed, security experts agree, is for tech suppliers to collaborate on implementing systemwide measures that protect consumers by default.

"Somehow, we need to find a way to let the good guys band together, and we'll all be a lot stronger," says Marc Willebeek-LeMair, chief technology officer at security firm TippingPoint Technologies.

Ed Amoroso, AT&T's chief information security officer, predicts: "There will be some set of catastrophes, then the lawyers will fight it out, and the question will come down to, 'Who's responsible if software flaws exploited over a network cause damage to society?' "

Russ Cooper, senior scientist at e-mail security company TruSecure, envisions a similar scenario: "It will take more calamitous events, perhaps an Internetwide attack that creates a huge public outcry, before regulators step in to protect consumers."



"They're not working together, and because they're not working together, they're putting all of us at risk."

— Alan Paller, research director of SANS Institute, about tech suppliers' Internet-security efforts

By Bill Perry for USA TODAY

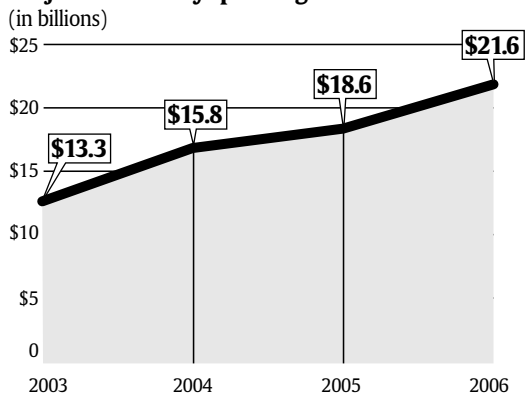
Cybersecurity spending to increase

Cybersecurity incidents

1999	9,859
2001	52,658
2003	137,529

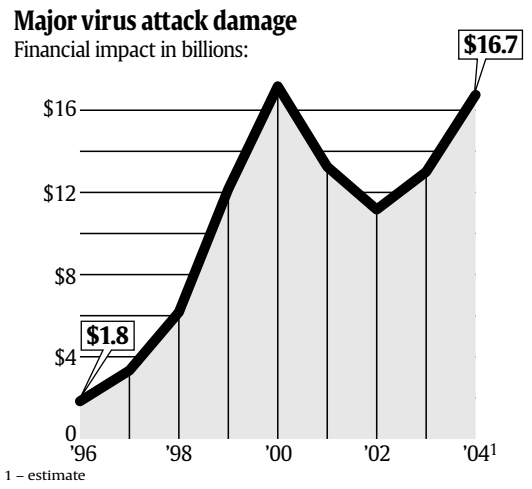
Projected security spending worldwide

(in billions)



Major virus attack damage

Financial impact in billions:



1 – estimate

Survey of 254 executives last spring reveals:

▶Computer viruses and worms are their biggest worry:

Share of executives citing these problems in 2004

Viruses/worms	92%
Hackers	50%
Accidental damage	40%
Spam	36%
Sabotage	27%
Denial-of-service attacks	17%

▶Many problems are caused by employees

Share of employees who:

Opened e-mail attachment from stranger	78%
Used name or birthdate as password for company network	29%
Accessed company network from public place and did not log out	17%
Shared company network password with outsider	9%

▶Both issues prompt an increase in cybersecurity spending budgets

2002	9%
2003	11%
2004	13%

Source: AT&T/Economist Intelligence Unit

Sources: CERT, Gartner Dataquest, AT&T/Economist Intelligence Unit and Computer Economics

By Alejandro Gonzalez, USA TODAY

Microsoft's SP2 won't cure all security ills

In the escalating cybersecurity war, Windows XP Service Pack 2, or SP2, represents a small advance for the good guys.

Microsoft issued its most security-focused software update Aug. 6. Experts recommend using it to enable a basic firewall and to access free Microsoft security patches. But SP2 might never reach many of the 210 million Windows XP machines already in use, because PC users usually ignore service packs.

SP2 does not apply for users of hundreds of millions of PCs running Windows 95, 98, NT, Me and 2000. Microsoft's advice to users of old versions of Windows: Buy a Windows XP machine with SP2 installed.

Amy Carroll, director of Microsoft's security business unit, says it's like replacing an old car with a new one equipped with anti-lock brakes and air bags. "Those kinds of things are very difficult to retrofit," Carroll says.

SP2 is notable for something else it lacks: anti-virus protection. Because the Windows operating system runs 92% of the PCs connected to the Web, some in the tech industry wonder why Microsoft hasn't tried to supply a base level of anti-virus protection free to Windows users.

Doing so would be a quick way to raise the overall level of security, says Alan Paller, research director at the SANS Institute, a security think tank and training center. Microsoft "is the only entity with the market power to ensure safely configured PCs, and their failure to do so is scandalous," says Paller.

Instead, the software giant is taking steps to become another supplier in the already-crowded anti-virus retail market. Since purchasing Romanian anti-virus maker GeCad last year, Microsoft has been developing an anti-virus product to sell to consumers and businesses on a subscription basis.

"Customers and partners have told us that security is one of the most important areas Microsoft can be investing in right now," says Mike Nash, who directs Microsoft's security initiatives. "Anti-virus is a key part of our defense-in-depth approach to security."

By Byron Acohido and Jon Swartz

ISPs conflicted

Mark Childs was a happy America Online customer for three years until the day he couldn't log on to his account. AOL had pinpointed his PC as a spam-spreading zombie. Without warning, AOL scrambled Childs' password, blocking his access to the Web.

Anticipating a call from Childs, AOL had customer support staffers waiting to guide him through steps to reclaim his account and clean up his PC. "I had no clue until they told me my PC was spamming," says Childs, 46, a land surveyor in Buffalo.

Childs' experience provides a glimpse into the massive resources Internet service providers are pouring into a patchwork of security initiatives that often confuses and frustrates customers.

ISPs supply the Internet connection in homes and businesses. They make money selling bandwidth, the channels over which data zip around the Internet. They are acutely sensitive to cybercriminals stealing bandwidth to engage in malicious activity.

ISPs have invested hundreds of millions of dollars on anti-spam systems and partnerships to distribute discounted anti-virus software to home PC users. EarthLink, which markets itself as a security-centric ISP, guides subscribers to tools designed to squelch pop-up ads, spyware and phishing scams. But like all other ISPs, it does not mandate that subscribers clean up PCs before accessing the Web.

"We do everything we can to educate and encourage consumers about security, but we do not require it," says Linda Beck, EarthLink's executive vice president of operations.

Instead, AOL, EarthLink and others have launched manpower-intensive programs to watch for and shut down tainted PCs as intruders put them to work. Typically, the home PC user whose machine has been hijacked is left out of the loop until the ISP moves to curtail Internet access or e-mail services.

AOL, with 23 million U.S. subscribers, suspends thousands of accounts each day. The company has teams of specialists standing by to quell large virus attacks, which can quickly infect hundreds of thousands of PCs. Such large-scale attacks occur once or twice a month, says Brian Zwit, executive director of integrity assurance at AOL.

"There's a whole educational process we go through about cleaning up your hard drive, and running anti-virus and anti-spyware," says Zwit.

Deb Naybor, 47, a city planner in Buffalo, had to reclaim her AOL account after an intruder commandeered her PC to spread hundreds of pitches for financial services and prescription drugs. "It's all part of the price you pay to be online," Naybor says.

In a bind over costs

ISPs face a dilemma. They typically get $50 or less a month from each subscriber. As zombies and malicious attacks proliferate, sucking up bandwidth and disrupting PC performance, consumers don't call the phone company or Microsoft, they call the ISP. It costs $8 just to have a service rep pick up the phone, about $50 to roll out a service truck on a house call.

ISPs remain conflicted, says Elias Israel, general manager for hosted solutions at MessageGate. "They all agree they wish other ISPs would police their networks better," he says, "and they all seem to agree that they themselves can't afford to do much more than they're already doing."

Charter Communications, which supplies high-speed Internet connections to 1.8 million homes, is a case in point. At its Atlanta headquarters, it recently installed anti-spam hardware and software that take up four times as much floor space as the e-mail servers they protect.

Charter has instigated a painstaking yearlong process of banning all its residential customers from using so-called Pop3 e-mail services, such as Outlook Express and Eudora, that allow users to retrieve e-mail stored on a remote server. Such services use a certain Internet channel — Port 25 — which has become the most widely used channel for spreading spam.

Charter and other ISPs have begun taking steps to partially or completely block Port 25. Charter is also attempting to set up a referral service to hand off subscribers who need help cleaning up and inoculating their PCs to a certified local repair business.

The balancing act that ISPs and other tech suppliers are attempting is a delicate one, says John Dreiling, Charter's vice president of advanced services: "How do I put enough resources in front of this problem without creating a cost model so high that I price myself out of business?"

"There will be some set of catastrophes, then the lawyers will fight it out, and the question will come down to, 'Who's responsible if software flaws exploited over a network cause damage to society?' "

— Ed Amoroso, AT&T's chief information security officer

The convenience factor

When Mike Nash pondered what Microsoft could do to make the Internet safer, he pictured cybercriminals going after his Uncle Ken.

As corporate vice president of security, Nash directs Microsoft's initiatives to help consumers secure their Windows PCs. It bothered him that Uncle Ken remained puzzled about how to install an important patching tool. Nash realized Microsoft had to do more.

On Aug. 6, after more than a year of development, the software giant released something called Windows XP Service Pack 2, or SP2. While Nash views SP2 as a quantum leap, security experts characterize it as a step in the right direction — but one that falls short in many areas.

SP2 automatically turns on the Windows firewall: a program designed to protect the PC from unauthorized access via the Internet. It also makes it easy to activate a free online service, called Windows Auto Update, that automatically downloads the latest Microsoft security patches.

But the firewall SP2 turns on is a porous one. It can be easily tweaked, even turned off, by an intruder, says David Berlind, executive editor of ZDNet, who has tested SP2.

Crooks tend to pounce on weak defenses. An Atlanta man who neglected to restart his anti-virus and firewall programs — after turning them off to download software — not long afterward discovered his PC was being used to broadcast waves of spam, says tech consultant Kimberly West of SpyderWeb Technologies, who helped the man clean up his machine.

SP2 does nothing to stop most types of spyware that get installed when a PC user unwittingly surfs to a Web site riddled with such contagions. Spyware can add unwanted links to a favorites list, change the default home page, steer users to porn sites and dial-down privacy settings to let more spyware in.

In July, spyware turned Ed Kemmerling's Web browser home page into a search engine for porn and online dating sites. It took the 57-year-old manufacturing consultant from Brighton, Mich., several hours to reformat his hard drive. "You can't even use the damn computer anymore," he says, "It seems someone is always spying on you."

Microsoft recommends using free anti-spyware programs — Lavasoft's Ad-Aware or Spybot Search & Destroy — created and maintained by volunteers.

Security experts unanimously recommend using SP2, because it brings XP computers fully up to date with all of Microsoft's security patches. But Berlind and others caution that its limitations could mislead consumers into a "a false sense of security."

Nash contends that Microsoft is doing all it can "to harden our product and make it as secure as we can."

The anti-virus question

By keeping vigilant watch for fresh malicious code, anti-virus software makers play a pivotal role in defending the Internet. But anti-virus companies are making so much money from old-style detection systems, designed to screen for known viruses, that a transition to more intuitive technologies has been sluggish, critics say.

In the past decade, Symantec, McAfee, Internet Security Systems, and Trend Micro grew from nothing to a combined market capitalization topping $24 billion by supplying anti-virus software to a hungry market. Their business model: Be the first to spot a new virus and the quickest to update a client's clean-up tools and filters to immunize against the latest threat.

But intruders have gotten lightning quick at counterattacks. They can tweak viruses just enough to slip past the latest filters. Virus writers used to take weeks to come up with a variation, which anti-virus companies assigned a letter of the alphabet. The Bagel e-mail virus, which first appeared in January, has been updated so many times that it's running through the alphabet a second time. The latest version: Bagel.AP.

In the past few months, new systems from TippingPoint, MessageGate and Cisco Systems designed to spot any code exhibiting a suspicious pattern have burst on the anti-virus software scene.

Because the newer, intuitive filters prevent the spread of anything that behaves like malicious code — rather than reacting to known virus signatures — wide use of them could be a big step forward in cleaning up the Internet, proponents say.

But the mainstreaming of intuitive filters will take years, experts say. Anti-virus suppliers will have to invest millions perfecting the newer technology so it doesn't accidentally block legitimate data. It will take time to get them to de-emphasize their highly profitable old-style filters.

Most consumers get introduced to anti-virus software by computer makers who supply it on a free trial basis on new PCs. But many consumers, such as Richard Riecker, a 29-year-old San Francisco corporate attorney, don't realize they need to pay for an ongoing subscription once the trial period expires, usually after 30 to 90 days. Riecker let his subscription lapse and fell prey to a virus, losing valuable data. "I thought I was covered," says Riecker. He now subscribes to an anti-virus program that automatically sends updates to his PC.

Microsoft estimates two-thirds of consumers don't have a current anti-virus subscription. Without one, they stop receiving updates, and their PCs become vulnerable to the latest virus attacks.

Bleak picture

With no one stepping forward to define and enforce some basic rules of the road, and with cybercrime flourishing, it's hard to find anyone in the tech industry to dispute the notion that Internet security will deteriorate, at least in the near term.

"It's a pretty bleak picture," says MessageLabs security analyst Natasha Staley. "There's a general lack of confidence and an overriding belief that things will get worse before they get better."

Most industry executives, when pressed, concede that market forces likely will have to emerge to compel Microsoft, Internet service providers and anti-virus companies — all of whom are already pushing hard — to embrace an even larger burden for securing the Web.

"Our customers own their computers, and what they do with them is somewhat out of our scope of business," says Mary Youngblood, EarthLink's customer security strategist. "Our responsibility is to make sure they have the best Internet experience possible, and we already have strong policies, dedicated folks, and strong products in place to address the problem."