



[Subscribe to Globe](#)

TODAY'S PAPER TECHNOLOGY

[Tech Home](#) | [e-insider](#) | [Reviews](#) | [@Play](#) | [Today's Paper](#) | [Investor](#)

[Tech Events](#)

Breaking News

- [Tech Home](#)
- [e-insider](#)
- [Reviews](#)
- [@Play](#)
- [Gift Guide 2003](#)

Security surges

The cost of protecting corporate computer systems is growing rapidly, yet many e-businesses still fail to take basic measures to protect themselves

By Kevin Marron
Friday, October 31, 2003 - Page 131

- [E-mail this Article](#)
- [Print this Article](#)

[Sign up for Tech Alerts](#)

Would you welcome the opportunity to make small purchases by waving an electronic card by a scanner instead of using cash or credit at the register?

- Yes
- No

[Results & Past Polls](#)

[Gift Guide 2003](#)



Find the perfect present for techies on your holiday list.

Advertisement

- [Encyclopedia](#)
- [Tech Alert](#)
- [Tech Books](#)
- [Tech Events](#)
- [Troubleshooter](#)
- [Special Reports](#)

In August, e-businesses everywhere got a series of wake-up calls from the dark side of the internet. It was the season of the worm.

First came Blaster, a crafty, virulent piece of malicious code that sneaked through a security hole in Microsoft software. Unlike viruses that attach themselves to e-mails and become active when users open them, worms move stealthily through the innards of computer systems without any human intervention. All told, Blaster infected 336,000 computers within 24 hours, replicating itself in a further 30,000 computers every hour, according to the U.S. clearinghouse for computer security, the CERT Coordination Center at Carnegie Mellon University's Software Engineering Institute in Pittsburgh.

[Technology News](#)
[Tech Investor](#)

- [Biotechnology](#)
- [Companies](#)
- [Gaming](#)
- [Hardware](#)
- [Internet](#)
- [Software](#)
- [Wireless](#)

Blaster was followed by Welchia, a supposedly benevolent bug designed to close the security hole that Blaster was exploiting. But the unwanted cure proved worse than the disease and, as a result, networks were slowed to a crawl. Meanwhile, the internet was being infested with a new epidemic in the form of SoBig.F, a virus that propagated itself through spam, getting into e-mail in-boxes and mailing itself to every address it could find.

[CCNMathews](#)
[Search Newswire](#)

- [Recent Releases](#)
- [Biotechnology](#)
- [Computers](#)
- [Software](#)
- [Telecom](#)

These bugs were more than just a pain in the neck for a handful of geeks: They caused disruptions to everyday life. Trains stopped running on CSX Corp.'s freight railway network, one of the largest in North America. Air Canada was forced to delay and cancel some flights when Welchia hit its phone reservation computer system. And, among numerous other examples of computer failures around the globe, perhaps the most sensitive and potentially damaging was a nine-hour shutdown of the U.S. State Department computer system that checks the names of visa applicants against a list of 78,000 suspected terrorists.



Advertising Info

**Advertise with The
Globe: Newspaper,
Web, and Magazine**

Services

- Newspaper**
- Corrections**
- Customer Service**
- Help & Contact Us**
- Reprints**
- Subscriptions**
- Web site**
- E-mail Newsletters**
- Free Headlines**
- Help & Contact Us**
- Make Us Home**
- Mobile**
- Press Room**
- Privacy Policy**
- Terms & Conditions**

All this serves as a reminder of how vulnerable our information systems are and the degree to which we depend on them. Richard Pethia, the director of CERT, told a U.S. congressional committee that Blaster has cost businesses an estimated \$525 million (U.S.), and SoBig.F between \$500 million and \$1 billion (U.S.). Even more disturbing is the fact that these attacks expose a broader problem with internet security. "Our current solutions are not keeping pace with the increased strength and speed of attacks,"

Pethia explained, "and our information infrastructures are at risk."

Businesses are spending more than ever before on security technology, and the cost of security is eating up a greater proportion of corporate technology budgets, according to Gartner, Inc., which reports a 28%-a-year increase in security spending since 2001, even though technology budgets have grown by only 6% a year. Gartner predicts that 20% of enterprises will experience a serious internet security incident-excluding virus attacks-before the end of 2005.

The problem, according to Pethia and other experts, is that organizations rely more than ever on on-line collaboration with customers, partners and suppliers, while employees frequently connect to corporate computer systems from home computers or through wireless networks. As corporate computer systems open themselves up to outsiders, there's a danger of letting intruders in.

What makes the risk even greater is that many computer programs are designed to be collaborative, and will therefore execute commands that are sent in remotely. What's more, the hundreds of computer programs used every day in various aspects of e-business each contain millions of lines of code, written by pressed-for-time programmers who rush to meet deadlines. The result: CERT reports that an average of 4,000 vulnerabilities-flaws that could create security problems-are discovered in software programs every year.

Whenever vulnerabilities are discovered, software companies act with haste to develop patches of code that will close the hole. Until now, they've succeeded in releasing these patches a year or more before anyone develops a worm to exploit them, but the most recent worms were developed within just 30 days of the vulnerabilities being found. According to Jack Sebbag, Canadian vice-president and general manager for computer security and network management company Network Associates, Inc., "These guys are a lot quicker to exploit known vulnerabilities and here's the scary part-they're also out there running all kinds of tools and code to see if they can find unknown vulnerabilities. These guys are good and they'll find stuff. They'll cause even more trouble."

When hackers discover vulnerabilities, they don't necessarily create viruses or worms that cause public mayhem, but will often use their knowledge for their own illicit purposes. For that reason, any company with information assets worth stealing should subscribe to a service that provides early warnings about all the known vulnerabilities.

Still, the largest threat of all arises when computer users and e-businesses fail to take measures to protect themselves. In almost all cases, the victims of worm and virus attacks could have protected themselves by installing patches and antivirus software that were available before the bugs attacked. As Ron Ethier, vice-president of technology at internet service provider Magma Communications Ltd., so succinctly puts it, "It's like everyone in your neighbourhood has their doors locked, but there's a criminal in the neighbourhood with a master key. Yet very few people change their locks."

Assessing the risk

Many companies fail to take security seriously until they're attacked, and some don't know what to protect

Although Norman Inkster has been chasing criminals most of his life, he'd rather get ahead of them. The former commissioner of the Royal Canadian Mounted Police, president of Interpol and security adviser to both the federal and Ontario governments is now a partner and head of risk management services at the law firm Gowling Lafleur Henderson LLP. His key piece of advice on information security issues: "If we're really interested in protecting ourselves in a considered way, we've got to recognize that bad people are always going to beat the system--and try to get a step ahead of them."

Shortly after Sept. 11, 2001, people listened to this kind of advice, and there was a flurry of activity around threat and risk assessment, as well as business resumption planning. But this activity has subsided. Instead of installing security features and upgrading them regularly to "keep ahead of the bad guys," Inkster says, "we put in a bunch of security features, wait until they're defeated and then correct them." Even though he preaches a proactive approach, he laments that most of his work is still reactive, as very few companies take security seriously until they become victims of a cyber attack.

The problem for many companies is that the risks are so immense and wide-ranging that they don't know where to start. As Dan McLean, a research analyst at IDC Canada Ltd., says, "Where companies really scratch their heads is that they recognize the magnitude of the threat that exists out there in terms of things that could compromise their IT. They recognize that they need to do something, but they're not certain of what they need to do or where they should start or what type of approach they need to utilize to really build out something that's ubiquitous."

Worse still, many companies simply don't know what they should protect. "A lot of companies are quite naive and ill-informed about the data they have and the value to the organization," says Mary Kirwan, a former federal prosecutor who's now an independent information security specialist. Corporate computer systems accumulate huge stores of data, ranging from their own trade secrets to confidential information about customers and suppliers. Losing any of this could have major ramifications for the company's reputation and its competitive position in the marketplace, not to mention legal consequences in the light of new privacy laws. Noting that a large percentage of corporate value is now wrapped up in information assets, Kirwan adds, "I'm not sure that companies in the past would have gotten away with not knowing what their physical assets were worth, but if you ask the same question about information assets, you get very vague responses."

Companies need to make an assessment of what information they store, where and what it is worth to them or to their competitors if it gets lost, and what it will cost the company if it's stolen or inadvertently disclosed. You can't protect everything, says Kirwan, so she advises assessing the key risks--threats from the outside and weaknesses in your own security--then "wrapping appropriate security around the crown jewels you want to protect."

But experts acknowledge that it's very difficult to put a value on security and figure out how much a company should spend on it, because it means calculating the cost of stopping something from happening. "This is what the industry is grappling with," says Kent Kaufield, senior manager in Ernst and Young's technology and security risk services practice. "How do you put a value on having a process in place that could stop the Slammer [worm] from shutting down your business for three days?"

When Cambridge, Mass.-based Forrester Research Inc. recently surveyed 50 top security executives at large global companies, nearly half of them said their budgeting process is flawed; 40% of them said they spend their security dollars on the wrong risks. Forrester's advice is to build your budget from the ground up--starting with a clean sheet of paper rather than with last year's budget--analyzing all the risks and considering both how likely they are to occur and how damaging they would be to the company if they did occur. Resources could then be focused on

preventing high-probability, potentially damaging events, while highly damaging low-probability risks could, perhaps, be covered by insurance and other risks addressed less vigorously, the Forrester study suggests.

For many small- and medium-sized companies, it's impossible to find the resources or the expertise to fend off the rapidly growing number of attacks and keep patching up software vulnerabilities, says Robert Offley, chief executive officer of Fusepoint Managed Services Inc., one of many technology providers that offers outsourced security services. "We can wear the pager and be there to do the security fixes, while they can focus on running their business," he says. This is a solution that much of the marketplace appears to endorse, according to Gartner, Inc., which predicts that 60% of enterprises will outsource monitoring of at least one perimeter security technology by 2005.

Kaufield and other experts think it's far less expensive to have a good security policy and appropriate technology in place than to be forced to spend money on reacting to events and new threats as they occur. The most important part of establishing a good policy is to get the highest levels of management involved. "Having a presence in the boardroom leads to things like appropriate budgets," Kaufield says, "and it also gives them some sense of what risks they are accepting by choosing not to put certain security measures in place."

Blame programmers

The software industry agrees: Robust design must take precedence over speed to market

Here's a lesson the technology industry has taken to heart: Software must get tougher.

"People are frustrated, not only in their experience with our software, but with the software industry in general," says Jill Schoolenberg, director of the Windows client group at Microsoft Canada Co., the Canadian arm of the software company that has borne the brunt of the recent spate of virulent worm attacks. "Certainly, we've all felt the pain and our customers have felt the pain a lot in the past few weeks. We've been working with them to see what we can do to make life a little bit better."

Microsoft programs have long been the favourite target of vandals in cyberspace, largely because its operating systems are the de facto standard for computer users worldwide. Despite the fact that Microsoft may be unfairly singled out, the recent spate of high-profile attacks "should be a wake-up call to some of these code writers," says Jack Sebbag, Canadian vice-president and general manager of Network Associates Inc., vendors of McAfee antivirus software.

Schoolenberg says her company is now responding to these concerns by undergoing what amounts to a major shift in culture. In the past, the software industry put a premium on speed to market and the rapid evolution of new features; now, the focus is on well-designed, secure programs. And when vulnerabilities are discovered, Microsoft has a policy of disclosing the flaw, making a patch available on-line and helping customers deploy it expeditiously.

At rival software giant Oracle Corp., where "Unbreakable Software" has become a marketing slogan, chief security officer Mary Ann Davidson says she works hard to encourage every employee to take responsibility for adopting top-notch security practices. Nevertheless, she says, there are

no "magic bullets" for making the software development process foolproof, and no good tools on the market

for automatically detecting errors

that can easily creep into millions of lines of programming code. "If you make a mistake--and developers do make mistakes--you're going to get whacked," she says.

The rising cost of defence spending

In 1988, the year the internet suffered its first major attack by a computer worm, the newly formed U.S. government-funded CERT Coordination Center investigated six cyber attacks. By 1998, the number of incidents reported to the agency had risen to 3,734. Last year, there were 82,094, and during the first half of this year alone, 76,404 attacks have been reported.

Given such bracing statistics, e-businesses are increasing their security spending incrementally. The total IT security market is growing at a rate of 25% a year, and is expected to expand to \$45 billion (U.S.) in revenues from \$17 billion (U.S.) in 2001, according to IDC, a Framingham, Mass.-based research firm. In Canada, companies are now spending more on e-business security, according to Dan McLean, a research analyst with IDC Canada Ltd., but he cautions that this increase is relative in light of the traditionally small amounts firms have spent in the past. "It would be hard to imagine firms spending less, because they frankly weren't spending a lot to begin with."

This year will mark the first time in history that more than 5% of IT budgets will be spent on security, according to Gartner, Inc., which measures the current annual growth rate of technology security spending at 28%.

Despite the fact that security spending accounts for a relatively small percentage of technology budgets, keeping e-business secure is a top priority for senior executives. According to Ernst & Young's Global Information Security Survey 2003, 90% of firms in Canada rated information security as essential to achieving their overall objectives. At the same time, more than 33% of those organizations said they were inadequately prepared to respond to cyber attacks.

The solution: vigilance

Staying ahead of hackers means constantly deploying new tools, such as software-vulnerability patches and antivirus updates

Hackers constantly prowl the perimeter security systems of Toronto-based Dynamic Mutual Funds Ltd., looking for holes in an electronic fence that protects the computer networks of a company that manages more than \$8 billion in assets for 350,000 investors.

"It's scary," says Gordon Bradshaw, the company's manager of technical services. So scary that he has an employee who does nothing but review logs of suspicious activity recorded by an intrusion detection system. Most illicit scans are unsuccessful; what really concerns him is "when they start coming over the fence."

Staying on top of security in today's risky, complex world of e-business requires sophisticated tools for managing these threats, be they early-warning systems that track newly discovered software flaws or integrated security suites that reach out to protect employees' home computers from viruses and hacker attacks.

The challenge is that any company doing business on the internet must be able to let outsiders into its networks, along with employees working off-site. This obviously entails opening up ports--doorways to the network--that hackers, worms and viruses can sneak through. Elesh Kadakia, systems marketing manager at networking products vendor 3Com Corp., says an effective security system should provide three levels of control that respond to three basic requests visitors might make: "Can I

come in? Once I'm on your network, where can I go? Now that I have access to your system, what can I do?"

Keeping out hackers is a never-ending battle, according to Bradshaw, who successfully fended off three major onslaughts during the height of last August's worm and virus attacks. "I think it's going to get worse before it gets better."

Tony Fernandes agrees. As vice-president of technology infrastructure at Inventure Solutions Inc., the infotech subsidiary of the VanCity credit union, he's responsible for maintaining security for an organization with more than 286,000 members and \$8.2 billion in assets. Like Bradshaw, he deploys a layered security system designed to keep intruders at bay without impairing network access for

customers and employees at 40 different branch offices in British Columbia. And he's feeling the pressure this year to handle a myriad of security threats because "the hackers are out in full force."

Keeping ahead of hackers means continually deploying patches for the vulnerabilities that software companies announce on what seems like a weekly basis. Businesses are often criticized for making themselves vulnerable to attacks by failing to install new patches quickly enough, but Fernandes says that deploying a new patch in a large, complex organization is not a simple task--and can sometimes even create more problems than it solves.

He points to a process he went through when Microsoft issued a bulletin describing a newly discovered vulnerability in its operating system. The patch deployment tied up four of his staff full-time for four days. First, there was a risk analysis to determine how critical the vulnerability was and how quickly the patch should be deployed. Then, the patch had to be built and tested to make sure that it would not create any unforeseen problems in interfacing with all the other components of VanCity's technology infrastructure. Finally, it was slowly pushed out to more than 2,000 computers in the network, while being closely monitored for glitches to ensure that nothing upset the finely tuned e-business network. Complicated stuff.

Antivirus programs must also be updated on a regular basis, a relatively simple automated process, except in situations where someone takes a laptop out of the office. Fernandes says this created problems last summer when an employee connected his machine to his home internet service, then returned from his vacation with a virus that "sent a lot of garbage into the network and slowed things down." With good security systems in place and expert staff, the problem was detected within 10 minutes and fixed within a half-hour.

Still, these activities are both time-consuming and expensive, especially since laptop use is becoming so commonplace. "The increased threat this year has actually eaten up a lot more of our resources than in previous years," says Fernandes. "There's been such a rash of them, especially in the past six months. It's something that you can't ignore, so you respond to it and some of your other projects end up slowing down. If the trend continues, or even if it stays at current levels, we'll have to plan for and budget for resources that won't be available for other things."

The other option: Your company could grind to a complete halt.



 [E-mail this Article](#)

 [Print this Article](#)

[Subscribe to The Globe and Mail](#)

[Sign up for our daily e-mail News Update](#)

[Back to the Search Results](#)

[Home](#) | [Business](#) | [National](#) | [International](#) | [Sports](#) | [Columnists](#) | [Entertainment](#) | [Tech](#) | [Travel](#) | [Cars](#)

© 2003 Bell Globemedia Publishing Inc. All Rights Reserved.

[globeinvestor.com](#)

[globeandmail.com](#)

REPORT ON
BUSINESS
TELEVISION

[workopolis.com](#)

[CTV.ca](#)

[TSN.ca](#)


Bell
Globemedia