

	<b>Download and Test Drive TurboTax Now!</b> <b>FREE!</b>	<a href="#">Click here to Download a FREE Trial</a>
---	--	---

To print: [Click here](#) or Select **File** and then **Print** from your browser's menu

-----  
This story was printed from [Enterprise](#),  
located at <http://www.zdnet.com/enterprise>.  
-----

## The New Security Threats

By Michael Bertin, [Ziff Davis Smart Business](#)

January 15, 2001 9:00 PM PT

URL: <http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2669953-8,00.html>

Colombian or french roast? not exactly what you'd consider a pressing executive decision. But shockingly, most businesses spend more time and money on the coffee they serve than on protecting their company servers. "Our research shows that for companies with top revenue greater than \$100 million in the United States, they are spending, right now, \$213 of every \$1 million of top-line revenue on security. That's two-hundredths of one percent of top-line revenue," says Frank Prince of Forrester Research. A colleague of his came up with the coffee-over-security estimate a few years ago when he did some rough back-of-the-envelope calculations.

Granted, security spending has increased dramatically over the past couple of years in response to high-profile breaches like those affecting Microsoft, Yahoo, and scores of other companies. In fact, since 1999 the number of companies spending over \$1 million on security has doubled. But most companies still severely underinvest.

And chances are you're one of them. You rationalize it: You're not a \$100 million company. The Internet is so vast that the odds of someone targeting your company are minuscule. According to Chris Klaus, founder and chief technology officer of Internet Security Systems, that's exactly the kind of thinking that is bound to get you into trouble. "The reality is that in many cases the way the attackers work is not based on exactly who you are," Klaus says. "They do a scan of the entire network, and if you've got a lot of vulnerabilities, you appear as a big target. So even if you're not a big company, if you are very vulnerable, you become a much bigger target."

The key is staying out of hackers' crosshairs. And to do that you need to know the key risks facing your business. We'll show you the top threats today—and the surprising ones you'll face tomorrow.

### Target Practice

The most common security dangers generally come from outside your company. These include hackers that want to snoop around your network, vandalize your Web site, or even steal proprietary information. Ironically, as hacking tools get better, many hackers become less skilled—*script kiddies* they're called, because they simply follow a set of instructions that someone more tech-savvy wrote—but they are no less of a danger.

Identifying the security risks posed by outsiders is the easy part. Viruses, worms, Trojan horses, denial-of-service attacks, and buffer overflows are generally well-known schemes. But knowing exactly what you're up against is also part of the challenge. These popular threats have been responsible for the

most successful and highest-profile computer crime cover stories of recent lore.

The distributed denial-of-service attacks against Yahoo, eBay, Amazon.com, and E\*Trade, among others; the ILOVEYOU worm; and the penetration of Microsoft—none of these were based on insidious new technology. But that didn't prevent them from racking up huge damage: The Yankee Group estimates these highly publicized attacks will have an impact in excess of \$1.2 billion.

"The key mistake people make is that they think about it wrong," claims Bruce Schneier, founder and chief technical officer of Counterpane Internet Security and author of *Secrets & Lies: Digital Security in a Networked World* (John Wiley & Sons, 2000). "They think, 'How do I avoid the threat?' When they should be thinking, 'How do I manage the risk?' "

To illustrate the point, consider the most common security precaution taken by businesses: the firewall. It's software that sits at the perimeter of your network and provides access control. Whatever traffic is not explicitly permitted to pass through is denied entry.

And firewalls are pretty good at what they do. According to Greg Smith of firewall maker Check Point Software Technologies, "I think you have to assume that 'the firewall' is 99 percent effective. It's considered the front line of defense for all companies and it's recognized that if I am going to be online, I absolutely must have a firewall."

But the widely publicized distributed denial-of-service attack launched against Yahoo last year demonstrates how vulnerable a firewall can be. The culprits simply flooded Yahoo's network with so many requests that it effectively shut the network down, firewall intact. And short of identifying the ISPs from which the attacks originated and blocking that traffic, there is almost nothing you can do to stop these assaults.

Firewalls also failed to stop the proliferation of last spring's ILOVEYOU worm. That's because the worm entered networks as an e-mail attachment. Most firewalls are configured to allow e-mail and benign-looking attachments to reach their intended recipient. Your front line of defense isn't much good when potential dangers can easily disguise themselves as regular traffic—akin to a really good fake ID—and cruise right into the network.

Of course, security companies can quickly write and distribute fixes, but the worms can do a lot of damage in the meantime. In the scant few hours it took to develop a patch to defeat the ILOVEYOU bug, the amorous worm had copied and distributed itself to some 10 million computers. Experts disagree on the total damages, but estimates range from \$700 million to \$15 billion.

Another serious security issue is complacency. As Smith explains, "One of the problems is believing mistakenly that by simply installing a firewall they are protected. It's very dynamic. It's not something you take out of the box, install, then walk away from." There are always new types of attacks, new types of services, and new types of vulnerabilities.

In fact, one of those new weak spots, the virtual private network (VPN), is a hot-button security issue for most companies these days. As more employees connect to their office networks from home, they expose the company to attack. A VPN lets companies use the Internet as a secure pathway into their existing network. It's a boon for far-flung offices and employees, but it's also a potential risk.

"One way to think of a VPN is as a hole in the firewall. Someone with a VPN is allowed to tunnel through the firewall into the network," Counterpane's Schneier says.

If a VPN user has an always-on Internet connection like cable or DSL, it complicates things. His system is connected to the Internet and if it is unprotected (read: no firewall) it becomes an easy target.

For example, a hacker could plant a Trojan horse—a program that gets secretly installed—on that machine. Then the hacker could have his way not only with that computer but with your network as well. "He can connect to it," Check Point's Smith explains. "He can install software on it. He can rummage

through the files and basically take over parts of the machine so that when you connect to the corporate network, he has wide open access into that whole network."

This is essentially what the Microsoft hacker did. He planted a Trojan horse (a fairly well-known and easily defeatable one at that) on an employee's computer and was able to infiltrate Microsoft's network.

In the face of these risks, what should you do? First, start with the basics: a firewall. Our top choice is Elron Software IM Firewall, which has full support for VPNs and starts at \$1,495 ([www.elronsw.com](http://www.elronsw.com)). But don't stop there. As Schneier warns, "A good hacker will get in, period. You speak to anyone who does penetration testing and they will say they have never found a network they couldn't penetrate."

Furthermore, Internet Security Systems' Klaus says, "The majority of hacking cases we see, I'd say that over 95 percent of the ones we investigate, the attacks stem from very well-known vulnerabilities that could have easily been prevented." The key to prevention is to identify and assess the threats to your computer systems and develop a security policy to address those threats and their consequences (see "Security Policy 101," page 81). If you don't have the time or resources to deal with these issues, consider hiring a security consultant (see "Hired Guns," page 85).

Whatever you do, be realistic. Says Schneier, "People basically want to buy magic security dust. 'Sell me the thing that I can sprinkle on my network that will magically imbue it with the property of security.' It doesn't exist."

## Inside Job

Malicious outside forces can cost you plenty, but there's actually a danger lurking within your company walls too. While losses attributed to denial-of-service attacks are steep—one estimate from APB News figured that Amazon.com lost \$244,000 for every hour it was out of service—they're significantly less than the losses incurred by insider security breaches. For example, simple laptop theft accounted for about \$10 million in losses, while unauthorized Web surfing cost businesses almost triple that amount, according to the 2000 CSI/FBI Computer Crime and Security Survey. Put simply, employees, partners, and others who are already inside your company's security perimeters pose a big risk. These inside jobs deserve as much—if not more—attention because not only do they pose a risk in and of themselves, but they can also trigger external security breaks.

The most obvious vulnerability is simple physical theft. That includes employees taking home a Zip drive, slipping a notebook into a briefcase, or even stealing an entire server. It could also mean printing and taking home documents containing company secrets. In fact the CSI/FBI survey found that the biggest security losses, some \$66.7 million worth, resulted from theft of proprietary information. Take the case of the alleged Chinese hacker who stole information from his employer and sold it to rival companies for about \$83,000. The final damage? It cost the company an estimated \$8.3 million per month in sales.

Often, insider security lapses are not intentional. In fact according to the 2000 Information Security Industry Survey, 48 percent of insider breaches—such as infecting company equipment with viruses—are accidental. Kevin Mitnick, the well-known hacker that cost companies like NEC USA, Nokia, and Sun at least \$290 million over a two-year span, sometimes didn't have to hack at all to defeat computer defenses. Using what's known as social engineering he was often able to get people to give him their passwords or whatever he needed to break into a network.

Social engineering is essentially tricking someone into giving you the information you want. It can be remarkably effective because it hacks the most fallible link of the security chain—the user. Mitnick was so successful at social engineering that, as he testified to Congress, he "rarely had to resort to a technical attack."

Imagine an employee getting the following phone call: "Hi, this is Bob down in HR. I need to verify some payment records. Could you give me your password?" It sounds reasonable enough, especially if you work

in a large corporation. The target is running late for a meeting, so he coughs up his password without thinking twice. So much for your company's bulletproof firewall and secure log-in procedures. By the time he is out of his meeting, "Bob" has sold some company secrets to your biggest competitor for six figures.

As Schneier puts it, "Amateurs attack systems. Professionals attack people." Why spend hours scanning a network for weaknesses or trying to run through password strings when you can get your entry pass in one phone call? Even the Love Bug used social engineering: Because it contained the subject line "ILOVEYOU," people were enticed to open it.

To prevent this from happening you need to police employees, but treating them as potential suspects is likely to damage morale. Moreover, companies are usually loath to tell employees things that are patently obvious—such as "Don't give your passwords to anybody."

"Characteristically, the infrastructure issue—setting up the VPN so that nobody can sniff the data going across the connection—is in some ways the easier issue," notes Forrester Research's Prince. "And someone hacking into the Web site and putting up a picture of Mickey Mouse in place of the chief financial officer is a more obvious and personalized threat. So people react to those, but in many ways it diverts them from the much harder problem of designing business systems that are inherently more robust."

The answer? Education. And that starts with a security policy (see "Security Policy 101,").

## Next Big Thing

Like insider security lapses, the next generation of attacks won't have to defeat technology. Instead they will exploit its capabilities. We already had a glimpse of this last year: In the early morning hours of August 25, a press release went out over Internet Wire saying that Emulex Corporation, a Costa Mesa, California-based company that specializes in fibre-channel technology, was being investigated by the Securities and Exchange Commission. The document said that as a result of some accounting irregularities the company was going to have to restate earnings from the past several years—turning profits to losses. The release also stated that CEO Paul Folino was going to resign. The story was picked up by Bloomberg and quickly went out to other financial news services.

By the time Emulex senior vice president Kirk Roller walked into the office at 7:10 a.m., and a mere 40 minutes into the trading day on Wall Street, Emulex's stock had plunged from 113 to 68. "And by the time I walked from my office to the CEO's office we had fallen to 45," Roller recalls.

The thing was, nothing in the press release was true. If anything, Emulex was in fine shape (in fact, the company eventually beat its projected earnings for the quarter).

How could this happen? A former Internet Wire employee had cooked up a bogus press release intended to influence the stock price and sent it out over the wire. And because there is so much competition to be first with potentially important financial news, the story was picked up and had spread before it was even confirmed.

By the end of the trading day, Emulex's stock actually shot back up as high as 130 before settling back down to roughly what it had opened at. But the damage had been done: Despite it being a case of misinformation, the SEC decided not to reverse the trades made as the stock price plummeted, for fear of setting a precedent.

"This was so far beyond even when you think about your worst day at the office. It wasn't even on the scope at the time," marvels Roller. "It wasn't like it was a technical attack on our systems." The effect was staggering: Emulex's market cap dropped \$2.5 billion in literally a matter of minutes.

Since then, the company has put in place a variety of measures to prevent this from happening again—including 24-hour switchboard access and an increased communications contact list. But how do

you protect yourself from something that you can't even imagine happening?

Says Schneier, "The class of attacks that are coming, you won't think of the methodology the attacker will use, but you can predict what the attacks are. The attacks are cyber terrorists—and I'm just making these up—the attacks are cyberactivists, the attacks are petty criminals. Exactly how they will do their job, we don't know. And yeah, it will be the thing we don't predict."

Donn Parker of AtomicTangerine, a venture consulting company, has a different theory about what the computer crime of the future will look like. Basically, he predicts that as hacker tools get more and more sophisticated, they will become automated. So much so that actual hacking talent itself will become superfluous and ordinary computer users will be able to perform illegal actions, what Parker calls "possessing a crime."

Parker sees a future where an ordinary person could download a program—for example, one dubbed Get Rich—and simply enter in some basic info to trigger a Web crime. The program might prompt the user to enter an amount, say \$34,000, and *voila!* The next day the money appears in his bank account. On the other side of the world an accountant in Hong Kong might find his books out of balance by that same amount, but the malicious program would leave no trace on either end.

Parker estimates that we could see these types of crimes start to develop in the next year or two. Schneier thinks we are already there.

Scary stuff, to be sure. But by making your company less vulnerable you become less of a target in the first place. And there are basic steps you and your employees can take to protect your business right now. If you have proper authentication systems in place, for example, make sure they are not disabled. Ensure that your firewall is properly configured. Don't open unknown attachments or download unknown software. And, of course, back everything up.

"That's one to really emphasize for people—to think of backup and recovery as part of your security policy," warns Vincent Weafer, director of Symantec AntiVirus Research Center. "Because you want to make sure that if the worst does happen—you do get an attack—you can recover from that situation."

Schneier cautions that the security route you choose should reflect your business's unique needs. "If you are selling books, you'll have one profile, if you are selling fine jewelry, you'll have another, and if you're selling groceries, a third," says Schneier. "But more security isn't always better. The same thing applies to the Internet. There isn't any one thing everyone should do." For help with beefing up your company's security, check out the best Web security resources at [smartbusinessmag.com](http://smartbusinessmag.com).

Michael Bertin is a freelance business writer based in Los Angeles. Additional reporting by Harpreet Anand.

---

## Security Policy 101

One size doesn't fit all when setting a security policy. But for any business, the more detailed and specific the policy, the better the protection it will provide. Your policy should address these key areas.

**Computing Resources** This is a broad topic, and there are a wide range of abuses related to it, but your policy should identify and address what is tolerable and what the consequences are for violating the policy, including: Are your employees day-trading at work? Or running a small business, say, building Web sites on company time? What about Quake tournaments in the office? Even seemingly harmless actions can cause serious security problems.

**E-Mail** Determine what comes in and what goes out. Sophisticated attackers might be able to penetrate your network via e-mail and e-mail attachments regardless of what barriers you erect, but a good policy goes a long way toward reducing e-mail-associated risks. For instance, simply blocking all incoming mail

that has executable file attachments can greatly reduce vulnerabilities.

**Virtual Private Networks** You've gone to great lengths and expense to create a virtual private network. But if home users—telecommuters, go-getters working late from home—connecting to the network aren't secure, then they can unknowingly escort attackers right in. Set up a system of checks and balances in which home users can't have remote access unless their connections are secured.

**Passwords** One-quarter of respondents to the 2000 Information Security Industry Survey reported breaches from attacks using insecure passwords. Passwords need to be turned on in the first place. Then they need to be changed often. Of course, they also need to be protected. That means no sticky notes bearing passwords attached to computer monitors.

**Fraud** A firewall can't protect you from everything. Focusing on technology issues at the expense of other threats is a mistake. Losses to fraud last year were greater than those due to sabotage, insider Internet abuse and viruses.

**Physical Theft** Does your policy account for all the laptops that have been issued to employees? Ask the same question for any item of value that employees might be walking out with (inadvertently or not).

## **Sneak Attack**

High-profile hacks like denial-of-service attacks and the ILOVEYOU worm garner all the headlines, but the majority of security breaches happen internally. High-profile hacks like denial-of-service attacks and the ILOVEYOU worm garner all the headlines, but the majority of security breaches happen internally.

Percentage of respondents who experienced these breaches in the past 12 months:

Installation of unauthorized software 76%

Infection of equipment via viruses/ 70%  
malicious code 70%

Illicit or illegal use of systems 63%

Abuse of computer access controls 58%

Unauthorized hardware installation 54%

Personal profit use (gambling, etc.) 50%

Physical theft 42%

Electronic theft 24%

Fraud 13% Source: The 2000 Information Security INDUSTRY Survey1 smartbusinessmag.comFebruary 2001 new secUrity threats

## **After You've Been Hit**

It can't happen to you? Guess again. And when a security breach does occur you need to deal with it as well as the perpetrator. By thinking about the scenario before it happens, you'll be better prepared. Start with this series of questions.

1. How did they compromise my security? By figuring this out, you can probably prevent it from happening again. If you are lucky, the fix is something as simple as getting a software patch from a product vendor or changing some passwords.
2. What did they do? If all they did was deface your Web site, you got a break this time; a few tweaks to the HTML and things are back to normal. But what about more serious problems like, say,

erasing reams of proprietary code or database files? Do you have everything backed up? What if they stole intellectual property? That leads into the next and trickiest question.

3. What do I do about the perpetrator? Unfortunately, finding the guilty isn't always a sure thing. Good hackers are able to launder their identity and remain hidden, often being flushed out only after the attack is reported publicly. There are serious considerations to take into account when going after an elusive culprit. Publicizing attacks has not only enormous potential public relations costs but also real monetary costs. A financial institution, for example, might face huge losses if customers think their money or their records aren't secure. Or what if a company decides the publicity risk is worth it and goes after the hacker? It's possible that documents containing proprietary info that they have to provide the court might cause even greater security threats down the road.

## Hired Guns

Losing sleep wondering if your business really is secure? Bring in an expert to help put your mind at ease. Security consultants perform a variety of services including network analysis, risk assessment, policy development, and security installation, as well as testing and maintaining systems.

Think of hiring a pricey security consultant as a form of insurance. Even moderately sized businesses should consider it. Bringing in a consultant is only a starting point, though, as many security companies are moving toward what's known as managed security. Basically you outsource all of your security needs, from installation of security systems to updates and even real-time monitoring. This solution is becoming increasingly popular among large corporations that would rather concentrate on their core business than worry about some hacker overseas.

The right security consultant depends on the size of your business. For larger companies it can be as simple as contacting IBM Global Services ([www.ibm.com/services](http://www.ibm.com/services)), Accenture ([www.accenture.com](http://www.accenture.com)), or one of the other big shops that have divisions devoted to security. You can also go with a specialty outfit like Counterpane Internet Security ([www.counterpane.com](http://www.counterpane.com)) or Guardant ([www.guardant.com](http://www.guardant.com)). Modest-size companies have many options too, typically smaller consultancies or independent consultants. The trick is to find the right fit. For specific companies and contact information, try an online directory such as [www.security-online.com](http://www.security-online.com). Also check out the various expert exchange sites on the Web, such as [exp.com](http://exp.com), [guru.com](http://guru.com), and [freeagent.com](http://freeagent.com).

When shopping for a consultant, ask the right questions. What type of services does the company offer? Are they tech gurus who are comfortable with hands-on work only, or can they also help you roll out a suitable security policy that takes more strategic expertise? Do they have experience with your business's type of hardware and software? Will they provide ongoing support or do they specialize in one-time setups? The best way to find out is to ask for references from current and past customers; call them for a reality check. **photograph by Chad Holder**  
**ABOVE** The biggest mistake companies make? Security expert Bruce Schneier says they try to combat security threats instead of focusing on managing risk.

## Outside Threat

You don't have to be a household name like Yahoo or eBay to suffer damaging security breaches. Billions of dollars were lost to viruses, Trojan horses, worms, and denial-of-service attacks last year—the most common external security dangers. You don't have to be a household name like Yahoo or eBay to suffer damaging security breaches. Billions of dollars were lost to viruses, Trojan horses, worms, and denial-of-service attacks last year—the most common external security dangers.

Percentage of respondents who reported the following:

Viruses, Trojan horses, worms 80%

Denial-of-service attacks 37%

Scripting/mobile code attacks 37%

Protocol weakness attacks 26%

Insecure password attacks 25%

Buffer overflows 24%

Attacks on bugs in Web servers 24%

Source: The 2000 Information Security