

PROTECTING YOUR DATA

Whenever you turn on a computer, there's a long line of hackers, malcontents, vandals, and thieves waiting to break in. Here's how to fight back.

In partnership with:





With viruses, phishers, and identity thieves everywhere, it takes hardware, software, and people to protect a company's systems and information.

Whether you're at home, at the office, or on the road, it's a fact of online life these days that whenever you turn on a computer there's a long line of hackers, malcontents, vandals, and thieves waiting to break in. Some want to steal your identity or bring your system to a crawl, while others are looking to erase your company's data. We live in a world where e-mail can circle the globe in the blink of an eye. Cybercriminals

can break into your computer just as quickly.

The dangers of online crime speak for themselves. *Consumer Reports* estimates that during the past two years one-quarter of computers have been broken into; 17% of those report the loss of important data. That shows up on the bottom line, with the average business break-in costing something in the area of \$14 million, according to the Ponemon Institute in Palo Alto.

More to the point, with so much information about customers, corporate partners, and suppli-

ers residing on business computers and databases, every intrusion is a potential data disaster. Take the case of CardSystems Solutions, a transaction processor for major credit card companies. Despite what officials thought was an adequate defense against online break-ins, a hacker slipped into its network last year and made off with the personal information of an estimated 40 million customers. "Events like this are accidents waiting to happen," says Jim Reavis, executive director of the Information System Security Association (ISSA). "Those who ignore this aspect of business will regret it."

"Protecting computers and the data they hold from intruders is no longer an option," adds Reavis. ISSA, a global group promoting information security since 1984, counts 13,000 information-security experts as its members. "It's an absolute requirement of doing business today."

The Digital Castle

With crafty cyber-attackers devising new ways to break into computers as fast as new defenses are erected, the best approach to computer security is a series of layers. Think of every computer in an organization as the digital equivalent of a medieval castle that's protected by several rings of defense. The modern-day equivalent of the castle's moat is the network's firewall, which offers a first line of defense against intruders. Next, rather than building high stone walls to keep marauders out, businesses use sophisticated filtering software to secure their digital citadels. Finally, instead of a battalion of armed soldiers patrolling the castle grounds, each computer needs antivirus scanning software that's always on the lookout for intruders that were able to sneak through.

"As important as each layer is," says John Jones, CEO of St. Bernard Software in San Diego, "its value is in being part of a comprehensive defense that blocks intruders at every possible entrance." In addition to selling filtering software that stops dangerous e-mail attachments, St. Bernard offers products to keep surfers away from inappropriate websites, as well as programs for backing up key files and making sure every computer has the latest security software. Some of the organizations that use its products include Kyocera International and the City of South Lake Tahoe.

But computer security is more than hardware and software. "We believe in taking a comprehensive approach to security," says Weldon Kennedy, vice chairman of Guardsmark. "There's nothing that compares to a strategic plan that covers all the bases from hardware and software to the personnel required to make it work." With headquarters in www.fortune.com/sections

"In a very real sense, we have to protect people and computers from the dark side of the web."

New York City, Guardsmark has more than 155 offices worldwide. The company doesn't sell security software or equipment, but creates customized security plans for some of the world's largest companies.

"If it has anything to do with security, we do it," adds Kennedy. The company recently completed a security control center for a large multinational corporation and staffed it with personnel checked and trained by Guardsmark. Chock full of monitoring screens and alerts, company staffers—from a single location—can observe both the physical and digital integrity of its facilities worldwide. "Down the street or across the globe, it can detect everything from burglars to hackers," says Kennedy. "With so many dangers on the Internet, security is a 24-hour-a-day job."

Hazardous Working Conditions

While it's clear that the Internet has become an invaluable tool for marketing research, purchasing, and staying in contact with far-flung employees, it can be a hazardous place to work. The threats, from software meant to cripple a computer to criminals trying to steal company data, are many and varied. "In a very real sense, we have to protect people and computers from the dark side of the web," says St. Bernard's Jones.

Policies, rules, and directives stating what employees are allowed to do online and where they're allowed to go are a good start, "but that's not enough these days," adds Jones. "You not only need a good policy, but you have to stop employees from violating it." St. Bernard's iPrism does just that. A combination of hardware and software, iPrism has an extensive database with detailed information on more than 7.5 million websites. From pornography to music-download pages, the off-limits list is arranged in 63 categories so that security staffers can pick and choose what type of web surfing is acceptable and what is not. When an employee tries to go to a porn site or get a quick game of online Texas hold 'em, iPrism not only blocks the connection so that no inappropriate material is viewed or downloaded, but in

The Time for Urgen

War, terrorism, workplace violence, sabotage, theft . . . the list of security-related worries preoccupying today's executive seems to grow each year. Who can predict what looms on the horizon? It's easy to pretend that corporations cannot shield themselves from these threats. Publicized tragedies heighten vigilance: anthrax made people think twice about opening parcels, workplace shootings led to new focus on disgruntled employees, and the September 11 attacks united the nation in a fight against terrorism. Unfortunately, complacency seems always to return with time.

Do you compromise on security when it comes to protecting your family? Experts know that ***the more you do, the safer you are***. Workplace security is no different; only the stakes are much greater. A large corporation is like an extended family living in a huge neighborhood: the chance of something going wrong somewhere increases with scale and there are more lives and livelihoods at risk.

Not all organizations think about security in terms of its total cost—at their peril. Some corporate budgets measure the dollars spent on security personnel and equipment but ignore the costs of crime and terror—the human tragedy, the liability expenses, the legal fees, the public relations and crisis management costs, the increased insurance premiums, the lost revenue from business interruption, the shaken confidence of customers and shareholders, the devastation in employee morale. Consider one example: A terminated employee, heavily armed, gains unauthorized entry past a new and inexperienced security officer. A single mistake, and several minutes later, lives are lost. Just one such tragic incident can jeopardize the future survival of an entire organization.

When companies view security services as a commodity, that is what they get. Some purchasing departments often only look at the unit cost, selecting the lowest bidder. Many service providers, however, fail to include additional costs, such as health insurance, vacations and even training, in their rates—which the customer may not discover until the invoicing starts. Other companies compete by minimizing their investment in wages, training and employee screening. Transient hourly employees treat their jobs in a perfunctory way. With limited authority, security managers cannot invest in quality or innovation. And yet if a serious incident occurs, they take the blame for failing to bring in a quality provider. This vicious circle detracts from buying the necessary value and focusing on what truly counts in security—results.

Being serious about security is not just about employing more security officers or buying more technological equipment. It is about approaching security in a different, smarter way. It is about knowing the

backgrounds of one's employees and on-site contractors. It is about ensuring that the one person accountable for security also purchases security. It is about considering the realm of possible threats and developing proactive solutions. It is about forming vendor partnerships to give others a stake in ensuring that all that can be done is done. It is about a commitment to total quality.

No entity can be entirely immune from crime and terrorism. When organizations commit time and resources to an urgent focus on security, however, they can minimize risk and create tangible value. A thoughtful security infrastructure supported by dedicated, energetic employees offers a shield against attack and often surpasses the traditional call of duty: responding to an accident on the shop floor and saving an employee's life or detecting a mechanical malfunction that could lead to a plant shutdown. A strong security program also acts as a deterrent. According to reports published in a leading national newspaper, a murderous terrorist cased a sensitive public facility in California and found the Guardsmark security to be so tight that he selected different targets, shooting six people and killing one. The wounded included three children.

When we founded our company in 1963, we saw an industry that failed to focus on total quality. We sought to fill a market void by offering higher pay to employ and retain better people—offering a career, not a job. To support these professionals, we built an unmatched management team composed of former FBI and Secret Service officials, military officers, and leaders of law enforcement agencies, creating a unique think tank for a broad spectrum of security-related issues.

Whatever concerns our clients face—from routine loss prevention investigations to dealing with kidnappings and assassinations in distant lands—our men and women stand ready with the wisdom of experience, the ability to manage uncertainty, and an intricate network of valuable relationships. These crisis-resolution skills give our clients the confidence that their security provider can respond to any emergency anywhere at a moment's notice.

Never before has confidence in security been more critical. Homeland security has emerged as an unprecedented concern. The United States of America is engaged in a war against terrorists who want to attack Americans at home, and the nation must take immediate action to correct its greatest vulnerabilities. Unfortunately, some institutions and organizations have failed to demonstrate sufficient urgency, focus and attention to safeguarding against the heightened risk facing the entire nation. The threat is not restricted to high-profile cities such as New York and Washington, D.C.; in fact, tighter security measures in those municipalities may convince the enemy to seek softer targets in less-prepared areas of the country.

cy Is Now[®]

Increasing emergency preparedness is essential to minimizing casualties. The ability of the United States to strike back with swift, devastating force does not deter agents of terror. Consequently, local governments must receive assistance to prepare for attack and to improve the technological capabilities of our emergency response agencies. Similarly, every organization must not only strengthen its defenses to prevent an attack, but it must also prepare to manage the aftermath of a successful assault by training on-site emergency responders and developing partnerships with firefighters, police and medical professionals. Securing a facility so that an attack will either fail outright or produce minimally disruptive consequences at best will significantly decrease the likelihood of a future strike.

The world has changed. Complacency has never been wise, but at this time of increasing uncertainty, it has become outright dangerous and irresponsible. At Guardsmark, we realize that each of our employees is the critical ingredient in securing some facility somewhere. Who that person is, what that person thinks and how that person reacts may make the difference between calm and calamity. That is why we are committed to excellence in management, to continuous innovation, to organizational ethics and diversity, and to an unyielding focus on the customer. It all has to do with being serious about security. That is our mission. And we believe that is the mission that you need.

The time for urgency is now[®]

GUARDSMARK[®]

10 Rockefeller Plaza, New York, New York 10020
212 765-8226 or 800 238-5878 www.guardsmark.com

*Ira A. Lipman
Chairman and President*

addition the monitor displays a warning screen.

Half a world away, iPrism is battling improper downloads on the network of 1,500 computers and satellite communications links that Proactive Communications, based in Killeen, Texas, set up for the military in Iraq. Too much of the network's bandwidth was being siphoned off by soldiers using peer-to-peer networking sites, according to Marc Legare, Proactive's chief operating officer. "Every time we tried closing down an inappropriate use," recalls Legare, "it sprang up again." St. Bernard's iPrism shut down the inappropriate activity, and Proactive's network in Iraq now has between 25% and 45% more bandwidth available for legitimate uses. The bonus is that the danger of picking up a stray virus has been reduced. "It really helped us enforce the rules," adds Lagare.

Rules may be meant to be broken, but ignoring the rules can be catastrophic when using the Internet at work. "In an online world, there's no substitute for common sense," says ISSA's Reavis. "The lack of thought by a single employee can result in a lot of damage." Take the Department of Veterans Affairs (DVA) analyst who loaded a database containing the personal information of nearly 30 million military personnel onto his laptop computer. The computer was stolen from his home, exposing millions to potential identity theft. The agency estimates that it will cost between \$100 million and \$500 million to fix the problem.

"That behavior is a clear no-no at many levels," says Guardsmark's Kennedy. Guardsmark not only advises clients on how to secure a facility and its digital infrastructure but also will screen and train the staff needed to make it all work. Before it hires anyone, the company does an extensive background check, tests for drug use, and performs a standardized psychological appraisal. All told, the company rejects 50% of applicants. "All too often we find that most companies ignore the people side of security," he adds. "It's as important as the hardware and software—sometimes more important."

Do's and Don'ts of the CyberWorld

Online, it's better to be safe than sorry.

Although hackers, virus writers, and spam artists change their habits daily, they can be held at bay. Here, thanks to several leading IT security experts, are key techniques to avoid online trouble.

Don't open any e-mail attachment unless you know who sent it, and never set an e-mail program to automatically open incoming files.

Do back up computers as often as you can and make sure your security software is completely up to date.

Don't let your guard down, no matter how secure you think your computer and network are, and never download any program that you're not sure of.

Do avoid questionable online areas like peer-to-peer file-sharing sites and pornography. That's where the most troublesome programs come from.

An Inside Job

Securing the digital front against hackers is one thing. Turning a blind eye to the possibility of a worker sneaking out with a backup tape containing a customer list, e-mailing payment records, or putting a new product design on a memory key is yet another. According to the experts, data leakage is becoming an everyday fact of business life. "Inside jobs are the next frontier for security software," says Jones of St. Bernard, "and as dangerous as hackers breaking in."

All it takes is a single employee intent on stealing information to breach what appears to be a complete security system. Jacqueline Lawrence was exactly that kind of employee at the San Diego Water and Sewer Department. Early in 2006, after 16 years of service, she made off with payment records and personal data of an unknown number of customers. She not only used the data to fund an online shopping spree but also sold some of the information to others. She's now serving two years in prison, but all the records were not recovered, leaving customers vulnerable to attack.

Problems of this sort are bound to multiply as new uses for the Internet develop. With online telephone conversations, TV broadcasts, and even web-enabled

kitchen appliances, the future may seem like a digital utopia to some. To others the possibilities for cybercrime are disturbing, to say the least. Imagine your phone getting a virus, your TV divulging your credit card information to an identity thief, or your home alarm system suddenly being taken over by a hacker. "Each new online application is an opportunity for someone to sneak in a rogue program," says ISSA's Reavis. "Data is everywhere these days, and we have to protect it."
—Brian Nadel

Join us at CSI 33rd Annual Computer Security Conference & Exhibition November 6–8 in Orlando, Fla. Topics include: Risk & Audit, Awareness, Management, Forensics, Web Services, Wireless, and more. Visit CSI33rd.com for more info and FREE show pass.

GET THE LOWDOWN ON WEB FILTERING BEFORE CLICKING HERE.

Software-based Web filtering seems simple,
until you think about all the hidden costs:

1. Purchase a server to run it on
2. Purchase another server for reporting
3. Purchase an Operating System for each server
4. Install and configure the Operating Systems and Web filtering software
5. Maintain and patch each server monthly
6. Deal with conflicts between the Operating Systems and Web filtering software each time they arise
7. Call multiple vendors' tech support to resolve conflicts
8. Watch for missed packets that you can do nothing about
9. Pad your budget for renewal time

Here's all you have to do with the
iPrism Web filtering appliance:

1. Plug it in



iPrism's Pure Metal Advantage delivers the security,
performance, and value without all the complexity and added cost.

www.stbernard.com/fortune

1-800-782-3762



To the rescue.

