

As your business becomes more collaborative and global, the risks to your company's trade secrets rise proportionally.

Fortunately, there are new strategies to protect the data that allows you to compete.

# YOUR WORLD...

The call to Bob Bailey, an IT executive with a major government contractor, came on an otherwise ordinary day in October 2003. "Why are you attacking us?" demanded the caller, an IT leader with a Silicon Valley manufacturer. He wanted to know why Bailey's company had launched a denial-of-service attack against his network.

Bailey (not his real name), deputy CIO in charge of IT operations, was thrown. He spent the next several hours reviewing logs and profiling systems. He discovered that someone had taken over one of the company's servers and was using it to launch attacks against other companies in the valley.

After conducting a forensic review of the drives, Bailey learned that intruders had been lurking on two of his company's servers for almost a year. These hackers, who were traced to a university in Beijing, had entered the company's extranet through an unpatched vulnerability in the Solaris operating system. As far as Bailey could tell, they hadn't accessed any classified information. But they were able to view mountains of intellectual property, including design information and product specifications related to transportation and communications systems, along with information belonging

#### Reader ROI

- Why online IP theft is a growing global threat
- Strategies for protecting crucial corporate data
- How to craft an incident response plan

to the company's customers and partners.

"It was such a sobering experience," Bailey says, not least because three years earlier he had conducted a network security audit and patched every hole. But he hadn't done the same with the extranet.

Bailey will never know who hacked his servers. China's poorly defended servers are often used to launch attacks. He likes to believe that the culprits

were a couple of students who launched the DoS attacks out of boredom, grew bored with that and went on their ways. But he knows that comforting scenario may be wrong. It's just as possible that the intruders were after his company's IP. And they easily may have gotten it.

(CIO agreed to Bailey's request for anonymity in order to protect the identities of his company's business partners.)

#### Exposed

According to cybercrime experts, digital IP theft is a growing threat. Although precise numbers are hard to come by, the U.S. Department of Commerce estimates stolen IP costs companies a collective \$250 billion each year. And that number does not



# Hacked

BY STEPHANIE OVERBY

include hacked or hijacked information that goes unnoticed or unreported. The economic costs on a nationwide scale are impossible to quantify just yet.

Suspected state-sponsored espionage against the U.S. government has received the most publicity, thanks to the investigation of a series of coordinated attacks on federal computers dubbed "Titan Rain." The 2003 attacks may have been the work of a China-based cyberespionage ring that was trying to steal government information, according to articles published in *The Washington Post* and *Time* magazine in 2005. But companies in any industry may be vulnerable. As businesses increasingly collaborate with external partners and expand globally, they're also increasing their exposure to criminals—and possibly foreign governments—who may have more on their minds than scoring some Social Security numbers.

"There's a ceiling on how much money can be made by stealing identities," says Scott Borg, director and chief economist of the U.S. Cyber Consequences Unit, an independent nonprofit institute set up at the request of the federal government to examine the economic and strategic consequences of cyberattacks. "You can actually *steal the business*—its processes, its internal negotiating memos, its merchandising plans, all the information it uses to create value. That's a very large payoff."

Unfortunately, most IT organizations approach the risk to IP the way they approach all IT security: focusing on the corporate perimeter and developing security tactics and policies from the system level up. Instead, CIOs must take a top-down approach. What's required today is a counterintelligence mind-set that assumes someone, somewhere, wants your data, along with multiple layers of defense to thwart would-be cyberspies and respond when (not if) they get through your defenses. "There are wide-ranging attacks against commercial organizations," says Bill Boni, CISO of Motorola. "It's incumbent on organizations—be they governments or commercial enterprises or academic institutions—to understand what their crown jewels are and make sure they are protected commensurate with their value."

## What's Your IP WORTH?

Define the value of corporate data to prioritize security investments

**You may think you know** which pieces of your company's intellectual property are most valuable—and therefore most vulnerable to intellectual property theft. But you're probably wrong.

Even at Microsoft, which is known for zealously guarding its IP, "one of the hard things to do is to get business leaders to articulate what pieces of information are most valuable in running their businesses," says Jim DuBois, general manager of information security and infrastructure services for Microsoft IT.

To capture the information you need to plan IP protection, ask questions, says Bill Boni, Motorola's CISO. You might start by inquiring what information might let a competitor move ahead in the market or help a counterpart in a foreign company achieve personal gain. A good business intelligence department can use its data to help.

Once you've identified your company's critical IP, which controls and countermeasures you put in place may come down to how much you want to spend defending certain know-how. Because there's little accurate data available on the costs of IP theft, there aren't any concrete cost-benefit models to work with. Boni uses Motorola's own financial predictions. "You've already done a lot of financial analysis about the benefits of a product or service," he says. "You can use those to estimate the damage if that IP is lost or stolen."

The cost-benefit calculation comes down to the probability of IP theft times its consequences, says O. Sami Saydjari, president of Cyber Defense Agency, a security consultancy. "If there's a decent probability that attacks could cost you \$500 million, it might make sense to invest \$5 million," Saydjari says. "Without that expected loss, you can't make the business case." —S.O.

### The Global IP Threat Landscape

The most widely known cybercrimes have to do with the theft of customer information and credit card fraud. (For more about fighting financial fraud, read "How You Can Fight Cybercrime," at [www.cio.com/article/117201](http://www.cio.com/article/117201).) But the cost of lost customer information could pale in comparison to the long-term damage done when a hacker targets a company's critical IP, says Borg.

According to the 2006 Computer Crime and Security Survey by the FBI and the Computer Security Institute, theft of proprietary data and unauthorized access to information are among the four most common sources of loss due to cybercrime (along with viruses and hardware theft). Although the survey did not report any increase in losses due to IP theft, the authors note such costs are hard to measure accurately. Security experts assume,

however, that the losses are significant.

"We've seen a big shift in the last two years to more sophisticated, stealthy attacks," says Gartner VP and Security Research Fellow John Pescatore. Sometimes, he says, the aim is purely financial—hijack some data and get the company to pay you to return it; or steal a customer database and sell the personal identification to whoever will pay for it. "Other times, it's industrial espionage. And as people started to look at where those targeted attacks were coming from, they found they were coming from all over the world." Experts point to China, Russia, France and Israel as big players in this black market.

CIOs may be less aware of the threat to IP than to their systems, and therefore less prepared to protect the former. "Companies are thinking about worms and viruses, things that will not have very bad consequences and have always been wildly

exaggerated," says Borg. "Or they're thinking about ID theft, which attracts a lot of attention, even though the number of cases is remarkably low."

There's a difference, too, in the systems an intruder looking for corporate secrets may target. IP thieves "won't necessarily look at obvious financially sensitive areas," says Borg, thereby escaping detection. "They may be looking at technical data, controls systems, automation software." And the results of IP theft can be hard to see—a slow degradation of one's competitive position in the market may easily be attributed to other, noncriminal factors.

Until recently, the most conclusive public evidence that sustained industrial espionage has taken place in cyberspace has come from the military. Titan Rain was "the most systematic and high-quality attack we have seen," says Ira Winkler, author of, most recently, *Zen and the Art of Information Security*. Chinese hackers successfully breached hundreds of unclassified networks within the Department of Defense, its contractors and several other federal agencies. One Air Force general admitted at an IT conference last year that China had downloaded 10 to 20 terabytes of data from DoD networks.

But it's not just high-profile targets that are at risk. "The intellectual property needed to build a new type of safety restraint for an aircraft is just as important as anything else," says Howard A. Schmidt, former CISO of eBay and former special adviser to the president for cyberspace security.

IP thieves have targeted companies as diverse as retailers and high-tech manufacturers. In incidents nicknamed "the Trojan Affair," 18 Israeli executives from several companies were arrested for their involvement in an international computer espionage conspiracy that targeted competitive information from rivals including, in 2005, the Israeli divisions of Ace Hardware and Hewlett-Packard. Also in 2005, several executives from the software company BusinessEngine pleaded guilty to hacking rival Niku's systems to access its trade secrets.

Nevertheless, some companies are more exposed than others (see "How Vulnerable Are You?" Page 42). Large, distributed

organizations provide more opportunities for attackers to gain access to corporate networks, says Alfred Huger, vice president of engineering for Symantec Security Response. Historically, the biggest risk to IP has been from insiders. A few years ago, Motorola detected suspicious unauthorized activity on its network. Boni's security team traced the activity to an employee workstation, which contained a directory populated with a complete hacker toolkit. Under questioning by investigators, the employee admitted that he'd been asked by a competitor to hack into Motorola's systems to access sensitive IP; he was terminated.

In today's global economy, the number of insiders within any organization has increased dramatically if you count external partners among them. "Organizations

### The Counterintelligence Mind-Set

As hacking has grown more purposeful, the traditional IT security mind-set has failed to keep up. "There's virtually unlimited information to protect and unlimited supply of threat and vulnerability," says Motorola's Boni. And there are no easy solutions. "Risk management oversight over distant suppliers is an emerging art," Boni says.

The vast majority of IP loss incidents are simple errors: posting information to externally facing websites wrongly assumed to be protected or including confidential information in a reply to an e-mail that includes external recipients, says Boni. The most successful hacks, says Bumgarner, occur because attackers get lucky, stumbling across a vulnerability while scanning thou-

"If eternal vigilance is the price of freedom, continuous monitoring and preparation to respond quickly is the cost associated with global digital commerce."

—Motorola CISO Bill Boni

now have to deal with employees connecting from home offices, the local Starbucks and shady hotels," says John Bumgarner, research director for security technology at the U.S. Cyber Consequences Unit. "They also have to deal with business partners and customers having access to their networks via VPNs, dial-up connections and Web portals, any of which can be used to compromise the organization's resources."

It was a connection to these externally based insiders that got Bailey, at the government contractor, in trouble. "The extranets pose a problem because many of them are controlled by program managers for the benefit of the customer," says Bailey. "And that can make policy enforcement problematic." But the focus on pleasing the customer backfired. "There's nothing worse than having to call up your customers and say, 'Because of our negligence, we've compromised your proprietary information,'" Bailey says.

sands of IP addresses. But the most dangerous attacks are deliberate.

To defend against targeted attacks, Motorola uses traditional controls such as firewalls, intrusion detection tools, anti-virus software and digital forensics—but with a difference. "We're operating our information security toolkit with a counterintelligence mind-set," says Boni. Like the military, Boni assumes there's an enemy looking for an advantage and it's his job to outwit him. "Putting those tools together with an understanding of what is or could be of greatest interest to competitors allows a more granular focus on the data," says Boni, "not just on the network."

Boni partners closely with business units to attempt to forecast the risk to particular IP-related information. (For more on how to do that, see "What's Your IP Worth?" Page 40.) "Every product or service has market share and projected finan-



cial. We try to understand what pieces of information are the key contributors to that product or service and whether they are at risk to targeted attacks.”

More companies need to adopt this more nuanced approach, agrees O. Sami Saydjari, president of Cyber Defense Agency, a security consultancy. “They’ll hire white-hat hackers—doorknob turners who shake all your doors and tell you where they got in,” Saydjari says. “And the company will try to figure out where to close those vulnerabilities. That’s primitive analysis.” When Bailey, the government contractor, conducted penetration testing of his internal systems, the white hats delivered a five-inch-thick report of vulnerabilities. Bailey says he closed every hole, but he ignored the extranet. Nor did he have a comprehensive program for updating systems and installing patches. “The lessons learned from the exploit were not uniformly applied across the business,” says Bailey. “That was my mistake.”

While monitoring and patching of systems is essential to any security strategy, many CIOs and IT security professionals approach the task backward, says Schmidt. “The discussion always seems to be, Tell me where the threat is and I’ll secure that system,” Schmidt says. “You need to test systems for vulnerabilities before deploying, have a plan in place to patch them, and audit to see who’s doing what and where data is.”

Turning the traditional approach to security on its head can help IT organizations prioritize spending to protect critical IP. “You need to look at the mission of the organization from the top down as opposed to the bottom up,” Saydjari explains.

## Defense in Depth

Without a clear idea about which IP assets most need protecting, CIOs may put their security dollars in the wrong places. “Most large organizations have all done basic blocking and tackling—firewalls, antivirus products, et cetera,” says Amit Yoran, CEO of network forensics company NetWitness and former director of the Department of Homeland Security’s National Cyber Security Division. But as with cybercrime generally, perimeter defense goes only so far. Companies need a cyberdefense strategy that is multilayered with different types

# How VULNERABLE Are You?

Distributed, poorly defended organizations face the most risk

**If your intellectual property** is digital, you’re at risk for online IP theft. But there are varying degrees of exposure. “It has to do with how valuable a target you present and how well-defended you are,” explains O. Sami Saydjari, president of security consultancy Cyber Defense Agency.

The types of organizations that currently face the highest risk include:

- ▶ Large, globally distributed organizations
- ▶ Small to midsize businesses in niche markets
- ▶ Companies with foreign partners or that sell directly in foreign markets
- ▶ Organizations with decentralized IT
- ▶ Military or government organizations that rely heavily on contractors and suppliers
- ▶ Industries like telecommunications that supply critical national infrastructure
- ▶ Organizations lacking executive sponsorship of security issues, technical enforcement of security policies, adequate security monitoring or process/preparedness for dealing with security breaches

External partners, locally and globally, are a major source of risk. “You can spend millions on your own defenses,” says John Bumgarner, research director for security technology at the U.S. Cyber Consequences Unit. But attackers may find a way in through weak spots in the systems of customers or suppliers. As intruders’ sophistication increases, however, all organizations may face similar vulnerabilities. “With new hacking methods, if the information is not encrypted and it is very valuable, it’s at high risk,” says Alan Paller, research director for the SANS Institute. —S.O.

of protection at each layer.

One strategy, called “defense in depth,” derives from the military technique for slowing down rather than trying to stop the advance of an adversary. The model applies when the question is not if, but when, hackers will break in. “If you reinforce one area, [attackers] will look to another,” says James Lewis, director and senior fellow with the Center for Strategic and International Studies. “The job is to reduce the chance that they’ll be able to get in.”

On the network, defense in depth means traditional perimeter security is supplemented with advanced intrusion detection systems, segmented networks with tighter security around some information, demilitarized zones for public data and security audits. But a good defense-in-depth strategy takes its multilayered approach to people, processes and technology as well.

The approach enables IT security teams to get beyond dealing with hackers as if

playing a game of whack-a-mole and treat the problem more like a chess game, says Jim DuBois, general manager of information security and infrastructure services security for Microsoft. DuBois has worked at Microsoft for 14 years and lived through a public incident in 2000 when hackers, who *The Wall Street Journal* reported were traced to Russia, allegedly accessed some of Microsoft’s key applications and source code. (DuBois was not part of the security group at the time. A Microsoft spokesperson argues that the incident was not portrayed accurately in the media, but that it reinforced the importance of security controls and helped drive adoption of several projects, including smart cards for remote access and a public key infrastructure—which allows for the secure and private exchange of data in unsecure environments.)

“The thought process is no longer making sure nothing bad ever happens,” says DuBois. “There may be a bug in the Cisco



code or someone might misconfigure a device. If [attackers] get at that chess piece we left unprotected, what will we do?" Microsoft has moved toward host-based controls, meaning they protect the data on a device or a network. "You have to protect everything, not just important data. Controls are more onerous than they need to be," says DuBois. He wants to get more granular. His goal is to secure the data itself, not the hardware or applications in which it resides, with next-generation digital rights management tools.

### Classifying Information

Over the years, Microsoft has sought to increase protection of its source code. But sometimes it has done too much. "We found a lot of places where we had too many controls around code we'll actually give away for free on TechNet," says DuBois.

The right level of protection can be difficult to pinpoint, however. Too often organizations apply the same standards of security for everything. That leaves some less valuable data overprotected and some more critical IP relatively exposed. Not only that, says Borg, but when CIOs think about what to defend first, they'll often think of the company's most-critical systems, like ERP or customer databases. However, he adds, "that's usually not where the liabilities are created, because that's not where the company creates the most value."

Motorola has developed what it calls an enablement zone environment, which segments the network, allowing groups of systems and applications to share a set of targeted security controls. In this way, security controls are aligned with the risk to the information the systems contain, as well as with relevant regulations or contractual terms. The most intrusive security solutions—including digital rights management, virtualization of content (to prevent its propagation outside the controlled environment) and role-based identity management—"are only warranted on

breakthroughs," Boni says. He advocates revisiting the classifications often. "If eternal vigilance is the price of freedom," says Boni, paraphrasing Thomas Jefferson, "continuous monitoring and preparation to respond quickly is the cost associated with global digital commerce."

### Your Incident Response Plan

Another layer of defense in depth is being prepared when intruders strike. "The IT model for dealing with a disruption is to get that server back online as fast as possible," says Boni. But before that happens, he adds, ask yourself how important the contents of the system are, whether intruders saw any critical data and whether the attack might be meant to distract you from the real target.

Boni does a first-level analysis. If triage determines that the incident could have a high impact, or if it appears deliberate, it may warrant a more significant response than the vast majority of intrusions that can be addressed through analysis of log files and systems profiling (for instance, he may call law enforcement, and secure affected systems and servers for evidence). "Prudent incident response means planning ahead," says Yoran of NetWitness. "People need to know how to receive and interpret various clues and deduce [what] may have occurred or may be occurring."

Communication is also critical. "Incident response is still very siloed and technology focused," says Khalid Kark, a senior analyst with Forrester Research. For serious breaches, Boni brings in a cross-functional team that includes, among others, crisis managers, internal auditors, lawyers and HR to assess the incident and determine who needs to be involved in the response. Yoran suggests interacting with public relations advisers, user communities and vendors, where necessary.

When the problem is global, the challenge escalates. "It may require interface with the local or regional staff, [which], given language, time zones and differences in operating practices, may be more difficult to coordinate, even inside an organization," says Boni. "Establishing working relationships with federal law enforce-

Large, distributed organizations provide more opportunities for attackers to access corporate networks.

ment ahead of time also helps," says Yoran. "They regularly work these issues with foreign parties."

When it's time to pick up the pieces, Alan Paller, research director with the SANS Institute, pushes for root-cause analysis to determine which exploits the hacker used and what can be learned from that. That's what Bailey, the government contractor, did once he discovered his problem. After contacting law enforcement, making a full disclosure to affected customers and partners, and completing a forensic analysis, he moved to cover the holes in his data protection strategy. These included better procedures for installing patches. He also recruited a manager of information security, expanded her department and set up a computer incident response team. Among its activities, the team lurks on hacker boards to keep up with the latest exploits and conducts intrusion detection exercises.

Today, most important, Bailey fully appreciates the risks. That's the key for CIOs who must manage the growing threat to corporate knowledge, says Borg: "Simply appreciat[ing] the stakes.

"There's some very sophisticated hacking taking place—some of it state-sponsored—and they're going after IP," says Bailey. "We can never be 100 percent secure, but we've redoubled our efforts. It taught us a big lesson." **CIO**

Contact Senior Editor Stephanie Overby at [soverby@cio.com](mailto:soverby@cio.com). Send feedback to [letters@cio.com](mailto:letters@cio.com).

#### Intruder Alert

Learn more about **PROTECTING THREATS TO CORPORATE DATA** at [www.cio.com/topic/1422/Intruder](http://www.cio.com/topic/1422/Intruder).

**CIO.com**