



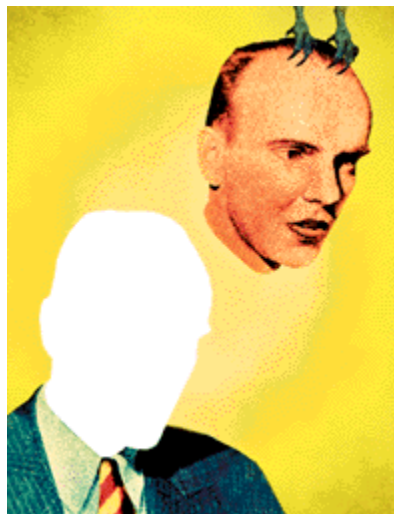
CSO

The Resource for Security Executives

csoonline.com | [Home](#) | [Magazine](#) | [Newsletters](#) | [Career](#) | [Online Features](#) | [Resources](#) | [Search](#)

April 2003 CSO Magazine

Intellectual Pro



Don't Lose Your Head

Intellectual property isn't always easy to identify. It's even harder to protect. Here's how CSOs can work with others to protect their companies' future.

BY SIMONE KAPLAN

PITY THE CSO. His worth is often measured by what *doesn't* happen on his watch. And he's often asked to protect things you can't see.

If you think it's tough to secure a building or a network, try protecting an idea. Ideas are invisible; they have a habit of working their way into conversations—and not always with the people who should be hearing them. They can get lost or stolen without anyone knowing they're even gone until your competitor beats you to market with an innovation you thought was yours alone.

Yet ideas are much more valuable than many of the tangible assets a CSO is sworn to protect. Intellectual property can be anything from a particular manufacturing process, plans for a product launch, a chemical formula or the names of the countries in which your patents are registered. In short, this kind of intangible proprietary information can amount to nothing less than your company's competitive future.

More and more, protecting such assets falls within the job description of the CSO. However, sometimes intellectual property ranks lower on a CSO's priority list than other security concerns, not because it is any less

■ IN THIS STORY

How to recognize and protect against threats to your company's intellectual property

Understanding the boundaries of IP and how it fits into the

CSO role

important but because it's just so hard to wrap your brain around. Intellectual property also varies from company to company and industry to industry. A CSO in the entertainment industry, for example, is not necessarily going to look at IP loss and theft in the same way as a CSO at a chemical company—so CSOs will approach protection of their companies' assets differently.

The upside is that IP loss, and how it happens, is predictable. Which means you can act preemptively. But IP protection requires patience and tenacity. Like everything else in life, it's not easy.

Understand What to Protect

Think of intellectual property as the lifeblood of an organization. "If a company loses its assets, it could die," says James Chandler, president of the National Intellectual Property Law Institute. Intellectual property comprises the principal assets by which a company is able to create its products or services. If those assets are lost or stolen, the company could lose its foothold in the marketplace. In fact, intellectual property theft costs U.S. companies about \$300 billion per year, according to Richard Isaacs, senior vice president at The Lubrinco Group, a risk management company.

Have something to say about this article? Add your comments below.....

The best way CSOs can protect proprietary information is by educating themselves and their employees about what their organizations hold valuable. If all employees understand what needs to be protected, they can better understand how—and from whom—to protect it. To do that, CSOs must communicate on an ongoing basis with the executives who oversee

intellectual capital. Meet with the CEO, COO and representatives from HR, marketing, sales, legal services, production and R&D at least once a quarter, if not more often, says John Pontrelli, director of security at W.L. Gore & Associates. "You must work in concert as a group to adequately protect IP," he says, emphasizing that such communication is an ongoing process, not a onetime event.

Once you understand your organization's products, research and intellectual capital base, and you've established a pattern of communication with other departments, then you've formed the base on which to begin to build an IP protection plan. CSOs who have been protecting intellectual property for years

Defining IP

To protect your company's intellectual property, you have to understand what is valuable to your company. To do that, you need to be able to define intellectual property for yourself.

[Read More](#)

recommend doing a risk vulnerability and cost-benefit analysis at this point. Make a map of your company's assets, noting which are considered the most valuable. Determine what information, if lost, would hurt your company the most. Then decide which of those assets are most at risk of being stolen.

It's What's Inside That Counts

Initially, it may look like most of the threats to your intellectual property are external, but that's typically not the case. No matter what your industry, intellectual property is lost or stolen in the same ways: insecure IT systems, disloyal workers or social engineering.

Whether careless, clueless or downright malicious, employees are the conduit through which IP is most frequently compromised. It's easy for employees to forget the role their work plays in the company at large, and they don't always remember that discussing a project at a cocktail party can put the company at risk. Business lunches and plane trips, in particular, are black holes for intellectual property—employees are talking to one person, while someone else eavesdrops or takes a peek at one of the employee's laptop screen.

Many employees have a hard time equating the importance of what they do with the long-term value of the company, says Lynn Mattice, director of corporate security for Boston Scientific's global operations. "They think they're working on a tiny part of a larger puzzle, so what's the big deal if they talk about it at dinner? You have to get them to understand the criticality of their job, how it fits into the larger picture and affects everyone in the company. Personalize it for them—make them see the personal impact of losing IP."

Sometimes, employees give away crucial information for personal reasons, without knowing it. For example, your industry may employ people with PhDs who, to stay certified, must publish field-related research. Often that poses a problem for employers that don't want proprietary intellectual property to become common knowledge. "We want them to publish," Pontrelli says, "but you can't allow them to talk about what they're working on because that would be of great interest to competitors."

Outside Looking In

Vendors and suppliers are always curious about what a company is up to, and employees are sometimes too willing to share that information with them. Engineers might enthusiastically explain a top secret project to a supplier just because the supplier asked about a certain part. You might work with outsiders on a regular basis,

**Keeping sensitive
corporate data safe**

from hackers is challenging, but how do you protect what is sent to remote desktops? Read "Securing the Corporate Content: Post Delivery Protection," a CSOonline ANALYST REPORT.

but they have no obligation to keep that information secret, particularly if they do business with competitors.

"There will always be people out there looking for weaknesses to exploit so they can get your goodies," says Jeff Uslan, director of information protection and security at Sony Pictures Entertainment. Even with good software and constant auditing, any method by which your company stores or transmits content has the potential to be infiltrated. "If you don't encrypt your information, that's it," says Uslan.

Another way in is through social engineering—calls from people posing as graduate students doing a research project or as ex-employees trying to track down a former boss. CSOs dub that kind of attack a pretext call, and even when employees know what's going on, they sometimes think they can handle it themselves. What they don't realize, says Mattice, is that they're dealing with trained intelligence professionals who use even tiny bits of information to construct a picture of what a company is doing.

The people on the other end of the hacks, social engineering penetrations and exploitations of employee knowledge are usually competitors or someone hired by competitors. Corporate espionage and competitive intelligence probes are the underground fraternities of the business world—knowledge of their existence is implicit, but no one likes to talk about them. They are, however, a big threat to the security of your company's intellectual property.

If you and your employees aren't on guard, your rivals could walk away with everything from your marketing plans to your deepest trade secrets. (*CSO* will cover this topic in greater depth in our May issue.)

Of course, there are those who will give away IP assets on purpose. Disgruntled employees walk out the door, and despite having signed nondisclosure agreements, find their way to the competition or form their own companies using your trade secrets. It's important to understand what factors contributed to someone taking information elsewhere, and how you could keep it from happening again. "You can't prevent everything," Sony Pictures' Uslan says. "But you can try to make sure that people see the consequences of breaking the rules."

“ There will always be people out there looking for weaknesses to exploit so they can get your goodies. ”

—JEFF USLAN, DIRECTOR OF INFORMATION PROTECTION AND SECURITY AT SONY PICTURES ENTERTAINMENT

Lessons from the Field

At W.L. Gore, intellectual property protection is crucial, and employee education lies at the center of the company's efforts. The company makes a chemical polymer that, when applied to outdoor clothing, produces the revolutionary wind and waterproof product known as Gore-Tex that hikers and climbers treasure.

Because W.L. Gore's business is built on such intellectual property, Pontrelli has created IP awareness presentations for employees at each of the company's 45 locations. W.L. Gore has many competitors, all of whom would love to get their hands on the company's proprietary information. And it's not just one person's responsibility to protect IP, he reminds them, it's part of everyone's job. Each employee is held accountable for his actions.

Employees sign a nondisclosure agreement (NDA) when they join the company, and Pontrelli underscores the obligation of sticking to that promise. He lets employees know how losing intellectual property hurts the company at every level. "We all rely on each other to protect our trade secrets," he says. "Maintaining the integrity of those secrets is the reason we're able to hand out bonus checks at the end of the year. So it affects everyone if something happens." Pontrelli also goes over the correct way to use technology to minimize the likelihood of data theft, such as using e-mail securely and saving electronic data in a consistent, safe manner so that no one outside the company can access the information.

CSO: The Resource for Security Executives

CSO Newsletters

CSO's free newsletter keeps you informed about the latest articles, analysis, news, reports and other developments at CSOonline.com. **Sign up today.**

Subscribe to CSO

CSO is free to qualified readers in the U.S. and Canada.

Read CSO Online

All the issues of CSO are available online.

W.L. Gore's engineers, technologists and PhDs receive a different presentation from the legal department that reviews the proper way to talk to vendors, suppliers and reporters, and how *not* to give out information. "Our employees are brilliant people, but when you put them on the phone with outsiders, they're not necessarily thinking about what they should or shouldn't say," Pontrelli says. "Unintentional sharing of confidential information is an area we address with regular IP awareness presentations. The litmus test for all of us to ask ourselves is, Would I know this information if I didn't work here, and would my biggest competitor want this information?"

I've Got a Secret

Four types of intellectual property protection

Read More

In 2000, W.L. Gore created an intellectual property committee to oversee communications with external entities as a major part of its efforts to safeguard its assets. If someone in the company wants to be quoted in a magazine, file for a patent or work with a new supplier, he has to go through the IP committee. "It's a

single point of review that prevents sensitive information from getting outside the company," Pontrelli says. W.L. Gore is divided into four large divisions, and before the IP committee was formed, divisions would often make decisions about what information could be released. "There was no consistent approach, and a division's business interest often dictated what information was released without consideration," he says. "The root of the IP issue is people. We had to find a way to influence the attitudes and behaviors of our employees so they would be more aware of the need for and ways to protect our intellectual capital."

As part of the IP protection effort, W.L. Gore now has a call information center, where employees can forward all inquiries about the company. The center's staff is carefully trained in the art of sniffing out social engineering attempts and answering questions without giving any confidential information away. Now, if someone receives a pretext call, it gets forwarded to the information center.

The best way to keep your IP inside the company, Pontrelli says, is to treat your employees with care and respect. "If you take care of them when they arrive and when they walk out the door, they'll respect the essence of the NDA; if you don't, the loyalty factor is diminished," he says. "Protecting IP is less about buying technology or hiring investigators to chase people. It's more about treating your employees right. If you make them not want to hurt you, you'll minimize your exposure. We can put up the biggest physical security barriers in the world, have the best IT systems and the tightest personnel screening program, but that won't stop a person from walking out the door with proprietary knowledge in his head."

Beyond the People

Uslan's mantra is audit, audit, audit. At Sony Pictures, his job depends on maintaining high levels of data security—particularly vital for industries such as his where large quantities of proprietary materials are electronically stored and transmitted. So it's not surprising that Uslan takes a vigilant approach to protecting Sony's internal IT systems. His department, which is part of Sony's information technology and protection organization, is the caretaker for all Sony intellectual property in digital form. "If it's on the computer, it's my job to protect it," he says. So he scrutinizes Sony's IT systems worldwide, testing every method by which his company stores and transmits content to make sure security is up to his team's high standards. He and his team are also regular practitioners of penetration testing, a practice that routinely turns up vulnerabilities that might otherwise

not have been found until someone outside the company had exploited them.

Uslan's audits resemble an ambush by friendly guerrilla forces. He and his team bring in a group of tactical IT security experts specializing in whatever operating system or software program Uslan is auditing at the time. (The company's network and systems administrators are extremely competent, he emphasizes, but their job is to keep Sony's systems up and running, not to analyze security—hence, the specialists.) The group of experts descends on each Sony location and begins auditing at the macro level, analyzing the company's servers and operating systems, checking for known weaknesses, and patching where necessary. Then it moves a step down, looking at every software program and every network port, testing as it goes. Afterward, Uslan meets with the network and systems administrators to tell them about any new problems or vulnerabilities discovered during the audit. "It's not an antagonistic event," he says. "We tell them what we found, how we found it, the tools we used and how they can patch the systems to prevent more holes from occurring. By the end, we've got them excited. And we've helped make both the systems and the administrators stronger." As soon as the group completes one audit, it's on to the next location to begin the process again.

Uslan understands why he needs to keep more than his finger plugged in the proverbial dike. IP loss affects everyone at Sony and beyond. "IP theft means revenue that we can't pass down to the script writers, the prop masters, the costume designers, all the people who work hard on films," he explains. "When someone gets a movie for free on the Web, for instance, instead of going to a theater, it's a slap in the face." He's also seen what happens when people get complacent about IP security. "It's when you think you've got all the bases covered that something big goes wrong. You have to stay on top of the process."

It's easy for CSOs to place the protection of ideas a lot lower on the priority list than protecting buildings and employees. Like Uslan says, CSOs get comfortable protecting what they know. Still, "intellectual property is what keeps your company viable in the market," says the National Intellectual Property Law Institute's Chandler. "And CSOs must make protecting intellectual assets one of their highest priorities." Nothing less than the future of your company depends on it. ■

Staff Writer Simone Kaplan can be reached via e-mail at skaplan@cxo.com.