MARKETPLACE

THE WALL STREET JOURNAL.

CUBICLE CULTURE

By Suein L. Hwang

Employees Try Out Inventive Weapons Against the Office Pest

IT'S IMPOSSIBLE TO avoid them: those well-meaning colleagues who lean over your cubicle and chat endlessly. They never take a hint, no matter how busy you look. For the modular masses, invading one another's cubicle space seems to be an inalienable right. Privacy is not.

Advocates of the open-plan office say it fosters communication and collegiality. In reality, open-plan offices, with their three-walled cubicles, tend to foster nosiness by their very design, emboldening co-workers to eavesdrop, intrude and interrupt in ways unimaginable.

But one person's nuisance is another person's inspiration. More than a few entrepreneurs have figured out that there is money to be made in helping employees regain control of their work environment. Faux cubicle doors, high-tech mirrors and other do-dads all promise some degree of privacy.

Sally Vitsky

Ai Architects, based in Washington, sells stacks of soft blocks in different shapes and colors called Protoblocs, which can be piled alongside cubicles to form barriers. By rearranging the blocks, workers can communicate to colleagues when it's cool to stop by (a green pyramid), and when to scram (a red square).

In 1999, Ai gave 300 workers at mortgage lender Freddie Mac some Protoblocs to test. Three years later, the soft colorful blocks are still around, but many workers have long grown immune to even a glaring red square. "If we need to speak to somebody, we disregard all signals," explains Eileen Moran, a graphics designer at Freddie Mac. "We just interrupt and go straight to the source."

AI'S RUSTY MEADOWS, the blocks' co-designer, concedes that Protobloc compliance is far from perfect. "Some people respected the system, some didn't," he says. "But when we asked people if they were willing to give them up the answer was 'absolutely not.' Even if it works only on some people part of the time, it saves an incredible amount of time and disruption."

Mr. Meadows says Ai has sold 15,000 sets of blocks ($14.95 for one; $10 in bulk) through its Web site so far, and orders are triple what they were a year earlier.

Some workers have gone a step further. Since 1996, thousands of cube dwellers have shelled out $20 for Cube-a-Door, made by Flexible Designs of Denver, Colo. It's a five-foot-tall cardboard panel that folds like an accordion and is emblazoned with the phrase "Please Do Not Disturb" in four languages. It's meant to be a fourth wall, enclosing the occupant inside a small fortress.

The barrier works—sometimes. "Some people just hang their head over the top," sighs Sandra Stierwalt, an administrative assistant at Raytheon who has one. "Do Not Disturb does not apply to everyone."

In the couple of years since she bought her Cube-a-Door, Ms. Stierwalt has found compliance has less to do with the panel than what colleagues believe is going on behind it. They steer clear if they think the person is working on something important. They barge in if they don't. When unsure, they peek over the top.

Privacy accessories are also subject to the law of diminishing returns. "The more they see it the more likely they are to ignore it," Ms. Stierwalt warns.

She says she uses her door "judiciously," unfolding it and closing herself in only twice a week.

CUBE-A-DOOR users say the door is virtually worthless when it comes to bosses. At StorageTek, based in Louisville, Colo., Web manager Shawn Fitzgerald recalls a time when a friend, exhausted from long nights working, put up his Cube-a-Door to take a nap, only to be awakened by his boss peeking over the top.

"Stronger language would definitely set a firmer boundary," Mr. Fitzgerald muses. "Maybe I need to upgrade."

Craig Dinan, a financial-services consultant and the entrepreneur behind Cube-a-Door, says he briefly toyed with selling a version imprinted with the words "p— off," but changed his mind after getting some negative feedback. He is, however, considering marketing a cubicle roof to resolve the peeking problem.

Plenty of other entrepreneurs have also discovered the cubicle privacy market. 3M makes a "privacy filter" that prevents nosy bystanders from seeing what's on your computer screen. In a recent Harris Poll poll commissioned by the company, 34% Americans admitted to sneaking peeks over colleagues' shoulders.

Lawyer and former dot-commer Chris Ryan is peddling a $19.99 Cubicle Survival Kit that includes ear plugs, a rear-view mirror, a fake window and cardboard signs that say "I'll Stop By" on one side and "Come Back Later" on the other. (The deluxe version, for $69.99, also includes a white noise machine.)

In my tests, I found the kit useful but only to a point. The earplugs allowed me to ignore colleagues only until they stuck their hand in my cubicle and tapped me on the shoulder. Monitoring the rear-view mirror to see who was approaching was even more distracting than talking to colleague.

The bottom line is, there are many ways to send colleagues a message that you want your privacy. Whether they will listen is another question.

E-mail me your own cubicle tales at cubiclecullture@wsj.com. To see past columns, go to CareerJournal.com.

Hiring a Hacker Brings Headache to a Security-Card Maker

By Bruce Orwall

TECHNOLOGY COMPANIES often co-opt troublesome computer hackers by hiring them. But as **NDS Group** PLC has learned over the past six months, such arrangements can be risky.

NDS, one of the satellite TV industry's top providers of antipiracy technology, is under legal attack by rivals who make the stunning accusation that the company has in some cases helped pirates steal TV signals. Last week, U.S. prosecutors in San Diego hit the company, a unit of media company **News Corp.**, with grand-jury subpoenas related to a continuing federal probe.

At the center of the allegations is 31-year-old Christopher Tarnovsky. In the mid-1990s, Mr. Tarnovsky was a notorious hacker who, under the alias "Big Gun," helped pirates decode the satellite signal of DirecTV, which used antitheft technology supplied by NDS. Looking to contain him, NDS hired Mr. Tarnovsky in 1997.

That solved a problem for NDS. But last March, **Vivendi Universal** SA's Canal Plus, a big satellite-TV operator in Europe, filed a lawsuit claiming that Mr. Tarnovsky continued to help pirates hack Canal Plus signals even after joining NDS. **EchoStar Communications** Corp., which runs the Dish Network satellite-TV service in the U.S., recently moved to join the suit, which was filed in U.S. District Court in San Francisco. The suit's status is uncertain as Vivendi recently agreed to withdraw it as part of another deal with News Corp.

Under Fire

NDS, a top provider of antipiracy technology, is under legal attack by rivals. Federal suits filed against it:

PLAINTIFF	AT ISSUE
Vivendi Universal's Canal Plus unit*	Alleges NDS helped pirate its satellite TV system in Europe
EchoStar Communications	Filed a motion to join Canal's suit, alleging the same happened to its Dish Network satellite system
Hughes Electronics' DirecTV unit	Alleges NDS engaged in fraud and misappropriation of trade secrets

*Suit may be withdrawn

Meanwhile, **Hughes Electronics** Corp., the **General Motors** Corp. unit that is the operator of the DirecTV network in the U.S., plans to drop NDS as a supplier and filed a sealed suit in U.S. District Court in Los Angeles against the company that alleges breach of contract, fraud and misappropriation of trade secrets.

The controversy has been a major headache for NDS, which makes "smart cards" that are designed to ensure the secure delivery of digital TV programming. The London-based company has seen its American depositary receipts fall nearly 80% since the allegations first became public last March.

NDS, which has denied the allegations, has stood steadfastly by Mr. Tarnovsky, and a high-powered legal team at News Corp., which owns 80% of NDS, is keeping a close eye on the situation. An attorney for Mr. Tarnovsky, Pamela J. Naughton, denies that he has been involved in any piracy-related activities since joining NDS.

Mr. Tarnovsky, who declined to be interviewed for this article, started his career as a satellite communications specialist for the U.S. Army based in Germany. Ms. Naughton, whose fees are paid by NDS, says he was a "gifted" computer hobbyist who, in his spare time, fiddled with satellite TV smart cards to learn how they worked. He also joined an Internet discussion group where he met elite hackers who discussed their efforts to defeat satellite-TV security systems.

After leaving the Army in 1996, Mr. Tarnovsky moved to New Hampshire and worked for a semiconductor company in Massachusetts. On the side, however, he worked as a programmer for a Canadian man named Ron Ereiser, who operated a business selling counterfeit smart cards that allowed people to receive DirecTV free. According to people familiar with the situation, when DirecTV and NDS deployed electronic countermeasures to disable counterfeit smart cards, Mr. Tarnovsky would program a fix that kept the bootleg cards functioning. These people say that Mr. Ere-

Please Turn to Page B8, Column 1

Why Airports Keep Growing

Longstanding Runway Plans Have Momentum of Their Own Despite Post 9/11 Slowdown

By Nicole Harris

ATLANTA—If Bill Hammack does his job right over the next two years, hardly anyone will notice.

The job? Supervising the moving of 27.7 million cubic yards of dirt to Atlanta's Hartsfield International Airport from land more than five miles to the south. Once it finally arrives, the dirt will be used to form a thick foundation for a new concrete runway intended to relieve congestion at the world's busiest airport.

PROPERTY REPORT

A look at Atlanta's dirt deal illustrates why runway projects continue across the country even as many airlines struggle to survive. In congested areas like Atlanta, the projects are so complex and controversial they take years to get off the ground. Even the disastrous effects of the Sept. 11 terrorist attacks aren't disrupting a five- to 10-year expansion plan when long-term forecasts still project an increase in air travel.

According to the Federal Aviation Administration, 18 major hub airports have proposed or begun building new runways at a cost of about $10 billion. But many of the projects require lengthy reviews by numerous city, state and federal regulatory agencies. San Francisco airport officials, for example, have spent $70 million over the past three years on research, planning and environmental studies just to see if they can start work to separate the facility's four runways, a delicate process given the airport's proximity to San Francisco Bay. In Louisville, Ky., the airport agreed to move a community of 540 homes away from the noise of its runways and to build a new city for the uprooted families. And in Seattle, airport officials are in their 15th year of planning a controversial third runway that will require three retaining walls to keep a 17 million-cubic-yard embankment out of a nearby creek and other wetlands.

In Atlanta's case, the plan is to move the runway dirt—enough to fill the Georgia Dome football stadium six times—without disturbing the environment or neighboring communities. A 5.5-mile-long electric conveyor belt will wind over streams, through woods and across five roads, including an interstate highway. To keep the dust down, the dirt will be sprayed with water and enclosed in covered bins. Two control towers equipped with video monitors will track the dirt's 30-minute trip to the construction site. Total project cost: $350 million, plus a $10 million bonus for on-time arrival by November 2004.

A 5.5-mile **conveyor belt** *carries dirt to Atlanta's Hartsfield airport for use in a new runway.*

Paving The Way

Eighteen major hub airports have proposed building new runways at a cost of about $10 billion. A sampling of some of the most costly projects proposed or under way:

AIRPORT	ESTIMATED COST
San Francisco International	$3 billion to $5 billion
Hartsfield Atlanta International	$1.3 billion
Lambert-St. Louis International	$1.1 billion
Seattle-Tacoma International	$773 million
Baltimore/Washington International	$600 million
Minneapolis-St. Paul International	$563 million
George Bush Intercontinental (Houston)	$260 million

Source: Federal Aviation Administration

The fifth runway project is part of a 10-year, $5.4 billion expansion of the airport, which served 75.8 million passengers in 2001. Once constructed, the runway will save the airline industry $5 million a week by cutting delays, says Benjamin DeCosta, the airport's general manager.

Like their counterparts elsewhere, Atlanta airport officials have endured opposition from local communities that didn't want another runway. They met their biggest challenge, though, when the dirt deal was mired in a nasty political scandal. C.R. Thornton, a local real-estate investor who owned the dirt needed for the construction and first proposed the conveyor-belt delivery method, pleaded guilty to making an illegal contribution to former Atlanta Mayor Bill Campbell. Mr. Thornton eventually sold his interest in the project to John D. Stephens, a local pipeline contractor who is now a subcontractor in the dirt project.

When the project was put out to bid early last year, a consortium of three companies known as 5R (for 5th Runway) Constructors LLP was the sole bidder, having agreed to use the conveyor method of getting the dirt to the site. After the City Council rejected the contract amid a public outcry over the contribution scandal, the price and the lack of other bidders, 5R sued in federal court.

In February, a court-appointed arbitrator

Please Turn to Page B4, Column 1

As Funds Fade, Symphonies Cut Their Programs

By Robert J. Hughes

ACROSS THE COUNTRY, financially strapped symphony orchestras are tuning up for fewer concerts, smaller-scale events and curtailed seasons.

The Cleveland Symphony Orchestra last month canceled its national radio broadcasts, a Sunday tradition since 1965, to combat a $1.3 million budget deficit. In Houston, the cash-strapped symphony cut its "Casual Classics" program, chamber music and two Mozart events, and last week it asked its musicians to take a 13% pay cut. And at the Milwaukee Symphony Orchestra, keeping on budget these days means "finding pieces that don't have huge numbers of extra musicians," says Steven Ovitsky, executive director.

Red Ink

U.S. symphonies with some of the biggest deficits:

INSTITUTION	DEFICIT
Philadelphia Orchestra	$1.3 million
Cleveland Orchestra	$1.3 million
Seattle Symphony	$719,000
Dallas Symphony Orchestra	$850,000
Milwaukee Symphony Orchestra	$500,000

Cultural groups often cry poverty, but this time is different. The funding environment has "taken a radical turn for the worse," says Marian Godfrey, a director of the cultural program for the Pew Charitable Trusts in Philadelphia, one of the largest arts grants-makers in the country.

Hard-hit by a switch in the way people buy tickets and by the falling stock market's effect on donors and endowments, classical music is facing its worst shakeout in years. Nearly a dozen cities' symphonies are operating six figures or more in the red.

The budget shortfalls have come, surprisingly, at a time when attendance is steady or even growing at some concert halls. The Philadelphia Orchestra and California's San Jose Symphony, for example, played to largely sold-out houses last year but still face million-dollar-plus deficits—calling into question whether the economics of high culture work anymore.

In the late 1990s, classical music seemed poised to pull in a whole new generation of fans. A booming economy led to ambitious program expansions, new concert halls and populist events that blended Bach with the Beatles. Attendance was 32 million in the 2000-01 season (the last one for which figures are available), up 16%

Please Turn to Page B8, Column 5

Scientists Say Lie Detector Doesn't Always Tell the Truth

Federal Agencies Should Halt Routine Use to Screen Employees, Prestigious Research Panel Says

By John J. Fialka

A PANEL OF SCIENTISTS say lie-detector tests that federal agencies have used for decades to screen for spies and other security risks aren't reliable, and new techniques should be pursued.

Little scientific basis supports the routine use of lie detectors on government employees, says Stephen Fienberg, a professor of computer science at Carnegie Mellon University in Pittsburgh who headed the panel. The group, in presenting its findings, concluded "national security is too important to be left to such a blunt instrument." Use of lie detectors by most private employers was outlawed by a 1988 law.

The 14-member panel, organized by the National Research Council, found that lie detectors, also called polygraph machines, are useful in criminal investigations where more-specific questions are used, but broader questions such as "Have you ever violated security rules?" often triggered false alarms. Innocent employees who worry more than most people about breaking rules, or guilty employees skilled at simple deceptive practices, may skew the results, the panel found.

Government agencies say they are taking the report seriously and studying it at length before deciding how to respond.

The panelists charged that scientific research into the polygraph hasn't advanced much since a Harvard psychologist, William Moulton Marston, first used fluctuations in blood pressure in an attempt to detect lying during World War I. Since the Cold War spy tensions of 1950s, however, the use of the polygraph for screening employees in federal intelligence and security-related government jobs has exploded, and tens of thousands of employees and applicants each year are subjected to such tests.

Skirting the Truth

Scientists say that subjects taking polygraph tests can lie more easily if the questions are broad, rather than detail oriented. A sample of problematic questions:

- Have you **released classified information** to any unauthorized person?
- Have you **committed sabotage**?
- Have you had any **unreported contacts** with a foreign government representative?
- Have you **concealed wrongdoing** by others that has damaged the agency?
- Have you spoken to any **unauthorized person** about classified information?

Frank Horvath, a criminal-justice professor at Michigan State University in East Lansing and spokesman for the American Polygraph Association, which represents more than 2,200 polygraph test administrators, agreed that the machine and the techniques for using it aren't perfect.

"The polygraph community has known for many years about the lack of adequate research, particularly in the screening area. It's really unfortunate that more hasn't been done to determine how effective screening really is," he said. He said, however, that current test methods should be retained until researchers find ways to improve them.

Modern polygraph tests involve measuring a number of bodily responses, including breathing, sweating and fluctuations in blood pressure that occur during questioning. The panel called for broader research into newer techniques, including measuring brain waves and minute changes in facial temperature. So far, though, it found, none of the newer techniques is as effective in spotting deception as the traditional polygraph. The panelists feel these areas might produce useful results if research were more robust.

"We stress that no spy has ever been caught by the use of the polygraph," said Kathryn Laskey, a systems engineering expert at George Mason University in Fairfax, Va. She and other scientists on the panel said the agencies that rely on polygraphs face a "difficult choice" between interpreting the tests too strictly and catching large numbers of innocent employees, or giving the results low weight and missing people who may be security risks.

The APA's Mr. Horvath said the largest users outside the federal government are police agencies, which use the devices to screen potential hires.

The National Research Council, an arm of the National Academy of Sciences, began studying polygraph testing at the request of the Department of Energy. Many of the agency's nuclear weapons scientists objected to the wider use of polygraphs in the wake of the Wen Ho Lee spy investigation. Mr. Lee, who reportedly passed a lie-detector test, was suspected of stealing nuclear-weapons data. He denied the charge and the government's case against him

Please Turn to Page B8, Column 3

INSIDE