The Virginian-Pilot

Serving southeastern Virginia and northeastern North Carolina

127th Year, No. 176

VOL. 7, NO. 41

HAMPTON·ROADS

JULY 27, 1992

BUSINESS WEEKLY

COMING OF AGE IN THE MIDDLE OF A SLUMP
PAGE 2

WHAT TO DO IF YOU'RE THE NEW MANAGER
PAGE 3

BATTERIES GET A CHARGE OUT OF THIS 'BUG'
PAGE 4

HOW COMPAQ HANDLES THE PC PRICE WARS
PAGE 10

Robert G. Cappello, left, and Martin Mongiello, operate Aegis Professional Security Services in Virginia Beach.

SPIES 'R' US

Some companies snoop on their competitors. Others keep a camera trained on their workers. It's not Big Brother though. It's just business as usual.

Robert G. Cappello, left, and Martin Mongiello, operate Aegis Professional Security Services in Virginia Beach.

SPIES 'R' US

Some companies snoop on their competitors. Others keep a camera trained on their workers. It's not Big Brother though. It's just business as usual.

JIM WALKER

LAWRENCE JACKSON

▲ "Information is the most valuable asset in business," says Martin Mongiello, left, president and engineering director of Virginia Beach-based Aegis Professional Security Services Inc. His partner, Robert G. Cappello, says surveillance can help a business pinpoint "poor management practices."

◀ Paul Van Auken, owner of Zero's Mr. Submarine shop in Virginia Beach, installed a video and audio system last month to watch customers — and workers. "Employees are basically honest," he says, "but it keeps an honest person honest."

STEVE HELBERMA

INSIDE

Ann Landers **B4**
Bridge **B5**
Classified **E1**
Comics **B4**
Crossword **B5**
Daily Break **B1**
Editorials **A6**
Friddell **D1**
Geske **D3**
Horoscope **B5**
Lottery **A2**
Local news **D1**
National **A2**
Obituaries **D2**
People **A2**
Sports **C1**
TV **B2**
World **A5**

TODAY'S CHUCKLE

Dairy diary: moo memoirs.

THE WEATHER

Cloudy with a chance of rain. High near 90. Complete weather/**A4**

Beware, the walls have ears – and eyes

Corporate spying is on the rise, using everything from pinhole cameras to hidden microphones. Story, **Business Weekly**

COVER STORY

Perils and profit in the spy trade

In tight times, more businesses snoop for scoops

By Phil Murray
Special to Business Weekly

PRICE WARS
PAGE 10

ia Beach.

US

etitors. Others
t's not Big
al.

LAWRENCE JACKSON

▲ "Information is the most valuable asset in business," says Martin Mongiello, left, president and engineering director of Virginia Beach-based Aegis Professional Security Services Inc. His partner, Robert G. Cappello, says surveillance can help a business pinpoint "poor management practices."

◀ Paul Van Auken, owner of Zero's Mr. Submarine shop in Virginia Beach, installed a video and audio system last month to watch customers — and workers. "Employees are basically honest," he says, "but it keeps an honest person honest."

STEVE WEVERKA

for at least 10 years. The operative's high-tech methods included bugging first-class sections of jets and snaring telephone and fax transmissions.

At the other end of the spectrum is "dumpster diving."

A discarded ribbon from a typewriter or fax machine, Mongiello says, can yield a wealth of information about a company.

"There is no question businesses spy on each other. You find less than is out there," says Chauncey, also president of the Virginia Association of Licensed Investigators and Security Services. "I think it's on the rise because the economy has tightened up. Why spend money developing something new when they can steal something already out there?

"But every businessman doesn't need to be paranoid that he's being bugged."

Though spies may use a lot of low-tech methods to gather information about a company, plenty of high-tech toys are also available.

Aegis' catalog of electronic gadgetry is a paranoid businessman's dream.

Take the recording briefcase.

The leather case offers state-of-the-art German engineering, the catalog says. The recorder is activated by removing a pen from its holder in the briefcase. All for $499. Pen included.

The case, Mongiello says, is very popular with businessmen who want to tape negotiations surreptitiously, which is legal. A less scrupulous executive might go to the toilet and leave the recorder running to find out what was said while he was out of the meeting room. That's illegal bugging.

The catalog also offers a wristwatch camera, $1,500; cameras hidden in smoke alarms, pencil sharpeners, clocks and plants — all more than $1,000; telephone scramblers to foil bugs, $299; and a "military intelligence countermeasures system" for sniffing out bugs and video transmitters, $1,995.

Heffernan cautions, however, that gadgets designed to locate wiretaps and other bugs are not generally effective against sophisticated equipment.

Mongiello, who founded his consulting and sales company six years ago in Charleston, S.C., also sells equipment to law enforcement agencies for sting operations and surveillance.

Mongiello says he has been in the military since graduating from high school nine years ago and has moved the company, first to Florida, then to Virginia Beach, when he has been transferred. He won't say what branch of the military he's in, or what he does.

"It pays the fellow to spend $500 to protect himself in a $40,000 to $50,000 negotiation," Mongiello says.

Improvements in technology that are making competitive spying easier are also finding applications in snooping on employees.

Companies that sell and install closed-circuit cameras for security say they are increasingly being asked to plant hidden cameras to watch workers.

Marc Rosenberg, president of B-Secure Video Surveillance and Security Systems Inc. in Virginia Beach, says he has installed hidden cameras in ceiling tiles and walls to try to catch employees stealing from the company.

He even put in a hidden camera for a businessman who wanted to keep watch on his partner. Rosenberg says he doesn't know what the man suspected his partner of doing. He doesn't ask a lot of questions.

That aspect of his business now accounts for about 20 percent of his revenues, he says.

"Stealing products and stealing money is more prevalent," Rosenberg says. "It's not so much stealing secrets."

Paul Van Auken installed a visible video and audio system a month ago to watch the front counter at Zero's Mr. Submarine, a shop he owns at the Great American Outlet Mall in Virginia Beach. Van Auken says he got the $1,700 equipment for security reasons, but has since found it a good tool for keeping an eye on his workers.

He can watch the work area on a monitor in his office, and each day he reviews the past day's tape of the times

Please see **SPYING**, next page

TOOLS OF THE TRADE

LAWRENCE JACKSON/Photo

A camera small enough to fit in a cigarette pack. Others masquerade as wristwatches or hide in smoke alarms.

A listening device, about half the size of a pencil eraser, can be planted under conference tables or behind lecterns.

A small tape recorder, popular with businesspeople who want to record negotiations secretly.

COVER STORY

Perils and profit in the spy trade

In tight times, more businesses snoop for scoops

By Phil Murray
Special to Business Weekly

Call it paranoia. But after losing several major clients to a competitor, a Virginia Beach wholesaler figured something must be amiss.

The competitor always seemed a step ahead, beating the wholesaler to the punch selling items in bulk to retailers.

Did the walls have ears?

Not exactly. But the table apparently did.

Security consultant Martin Mongiello found traces of tape on the underside of a table in a room used to make presentations to clients.

In one of the executive offices, he found an actual bug — a small radio-frequency listening device sold in local electronics stores as a wireless microphone for $29.95. Low-tech, but still effective.

The bug, about half the size of a pencil eraser, was in an "object" in the office; Mongiello won't say exactly where.

While corporate dirty tricks may not have been the only reason the wholesaler was losing business, Mongiello says whoever was listening had a big advantage.

"Information is the most valuable asset in business," says Mongiello, president and engineering director of Virginia Beach-based Aegis Professional Security Services Inc. "Without a doubt this is what crippled them. It set them back at least six years."

Welcome to the world of corporate espionage: pinhole cameras hidden in sprinkler heads or bookbindings, microphones in briefcases and umbrellas, covert operatives.

The stuff of spooks and cops is also readily available and, security specialists say, used more and more by businesses to spy on their competitors — and their employees.

Security firms in Hampton Roads say they are being called on more frequently to help companies keep secrets from walking out the door. They also are getting more business from companies interested in keeping closer tabs on their workers, either through electronic surveillance — both open and concealed — or by planting a spy in the work force.

Statistics are hard to come by, but one survey conducted last year by the 25,000-member American Society for Industrial Security in Arlington found that 37 percent of the companies responding had been the victim of a theft or attempted theft of company secrets.

The targets were largely new technologies and research: semiconductors, software, optics, pharmaceuticals. And the secrets were spirited away in a variety of ways: break-ins, insider theft, intercepting fax messages and telephone calls, computer hacking — even digging through the trash.

The survey was hardly exhaustive. Only 165 companies responded. But the man who conducted it for the group, Richard J. Heffernan, says corporate spying is much more widespread than business leaders realize.

Not only are there threats from domestic competitors, but foreign governments and businesses also get into the act to get an edge on U.S. companies.

"When an expert pickpocket is operating, you may see the wallet gone, but you wouldn't feel the touch," says Heffernan, president of R.J. Heffernan Associates Inc. in Branford, Conn., considered one of the top experts on corporate espionage. "When information theft is done by professionals, it's like somebody took the wallet and put it back before you knew the wallet was gone.

"It's very definitely a growing problem as people are looking for short cuts in the research path."

Though security specialists say corporate spying is on the rise, hard evidence is tough to come by.

Robert E. Chauncey, chief investigator for Associated Investigative Services Inc. in Portsmouth, says the only piece of eavesdropping equipment he's ever found was a radio transmitter planted behind a podium in a hotel meeting room several years ago.

He's discovered a telephone line run into an attic and phones that had been tampered with, but little else in the way of direct proof.

That's not for lack of looking, however. Chauncey, an investigator for 25 years, says he is contacted once or twice a month by a company worried about secrets being stolen.

The problem is that the methods of the corporate spy are not always so obvious.

Some firms assign employees to pore through government reports and other public documents to gather information on a competitor.

In less savory cases, employees can be bribed for information, or disgruntled workers can pass along secrets to get back at the boss.

A Merck & Co. employee in New Jersey was nabbed in 1990 by a sting operation when he tried to sell a pharmaceutical process to an FBI front company for $1.5 million.

Foreign spies, with more time on their hands these days, are turning their attention to corporate, rather than government, secrets, Heffernan says. The former head of a French intelligence service has admitted to spying on U.S. companies

SPYING

Continued from previous page

when he was not around.

The camera, Van Auken says, has helped the business become more efficient as well as deterring employee and customer theft.

"Employees are basically honest, but it keeps an honest person honest," Van Auken says. "With this they can't say anything but the truth. They can't hand me excuses when I've got their butts on tape leaning against a prep table for two hours.

"It stops all that."

Companies also keep an eye on their employees the old-fashioned way: by using real spies.

Robert G. Cappello, president of American International Security Specialists Inc. in Virginia Beach, says he has several "covert operatives" planted in companies in Hampton Roads and out of state who give reports to the corporate brass on the management of stores and branch offices.

Managers usually are duped into hiring a person who works for the security firm. That person then is in a position to be a company snitch.

Operatives typically look for theft, employees spending too much time on the phone, dancing in the aisles, sloppy money-handling procedures — anything that reduces productivity.

It's very common, says Cappello, a former Navy policeman and deputy sheriff for Virginia Beach who also is part owner of Aegis. "A store may be losing money because of poor management practices."

All this Big Brotherism, however, has prompted some concerns.

Federal and state law does not address the issue of hidden surveillance of employees. Notions of privacy in the Constitution are endangered by the high-technology spy tools used today, says Kent Willis, director of the American Civil Liberties Union of Virginia.

Willis says his office is investigating a recent incident at a Richmond hospital in which overzealous security people hid a camera in a women's locker room after a spate of vandalism.

A 1988 federal law regulating the use of polygraphs in the workplace was the first step in recognizing employee rights to privacy, Willis says. The next steps will involve regulation of substance-abuse testing and surveillance, he says.

"We get as many complaints on (employee privacy) as about any other subject," Willis says. "Employees who feel like they are being spied on at all points may be less effective as employees."

As the business of secrecy gets bigger, security firms themselves have to be wary of prying eyes.

Signs posted in the suite of offices shared by Aegis and American International advise visitors that they are subject to audio surveillance.

Security specialists also are careful about revealing too much about their clients and techniques. You don't have to tell these guys about loose lips.

"I know you might think we're paranoid," Cappello says, "but Marty shreds every piece of garbage in here."