

CANADIAN Electronics

VOLUME 12 NUMBER 6

THE NEWS AND PRODUCTS JOURNAL FOR THE ELECTRONICS INDUSTRY

SEPTEMBER 1997

FEATURE REPORT

THE BATTLE AGAINST TECHNO-CROOKS

By Joe Wilson

The attraction of the electronics industry and its stocks of high priced components for criminals is well known.

"There's been a dramatic increase in theft of electronic equipment and components," says Bob Lusty, detective with the Peel Regional Police Department just outside Toronto.

What is less commonly realized, however, is how the heightened security electronics companies have installed in response to their high threat levels has acted as a stimulus to criminal ingenuity.

The result is that burglar tactics have rapidly outdistanced the clumsy break-and-enters common only five years ago, and rendered conventional security systems all but obsolete.

Today, felons familiar with the failings of these systems which may include high tech access controls and glass break detectors, often

bypass normal modes of entry by doors and windows.

Instead, they execute Topkapi maneuvers crawling through ventilation shafts or chopping holes in roofs. Once inside, they may set off motion detectors. However, police responding to the alarm and checking the facility will find all secure.

The job at the electronics company bore the hallmarks of professional planning. Although the thieves were unsuccessful at evading the highly sensitive audio security system, they took every possible precaution.

First they entered the unoccupied offices on the second floor of the new building via the air-conditioning vents. Then they

chopped a hole in the floor to

access one of only two small areas on the main floor not equipped with audio sensors: the men's washroom.

When they found their way into the back area of the building barred by access control, they

returned to the washroom and cut a hole through the wall to the manufacturing and shipping area. Aware that this activity must have been picked up by the audio sensors, they made a fast exit from the customer pick up area.

Stealing to order is commonplace. Detective Lusty adds that although goods are usually impossible to trace, sometimes they show up unexpectedly.

With all this activity, and despite the very high apprehension rate of electronic thieves in certain regions such as Mississauga, it's no surprise the insurance industry is casting an increasingly jaundiced eye on the electronics business.

"Our research on loss prevention is finding a general lack of expertise and operational management in this area," says Sonya Fitterer, president of Paradigm Insurance Group which specializes in insuring computer and high value accounts.

"There's a move underway to address the products of the electronics industry much like gold or diamonds because losses in this sector greatly exceed those experienced by traditional manufacturing or service companies," Fitterer adds.

Looking at the source begins with knowing your enemy and planning accordingly. In the last 12 months, Sonitrol audio security assisted in capturing a high percentage of the criminals attempting to burglarize electronics firms it protects (approximately 80 felons in 60 events).

The typical profile of those apprehended includes: mid 20s to 30s, highly articulate with a relatively high education level, from a middle class background, and usually affiliated to one or more semi-organized gangs. Because of the difficulty of these kinds of crimes, thieves often work in pairs. They typically scout out locations and plan their crimes over a period of weeks.

Against this smart, brash and technologically adept criminals willing to take enormous risks for high stakes, only detailed, imaginative security planning and the most effective counter-measures will succeed.

Retired Toronto police sergeant Tim Hilton points out a key consideration when he says "security is like an onion, and involves multiple layers of protection."

Joe Wilson is vice president, Canadian operations at Sonitrol.

Circle CE 435

