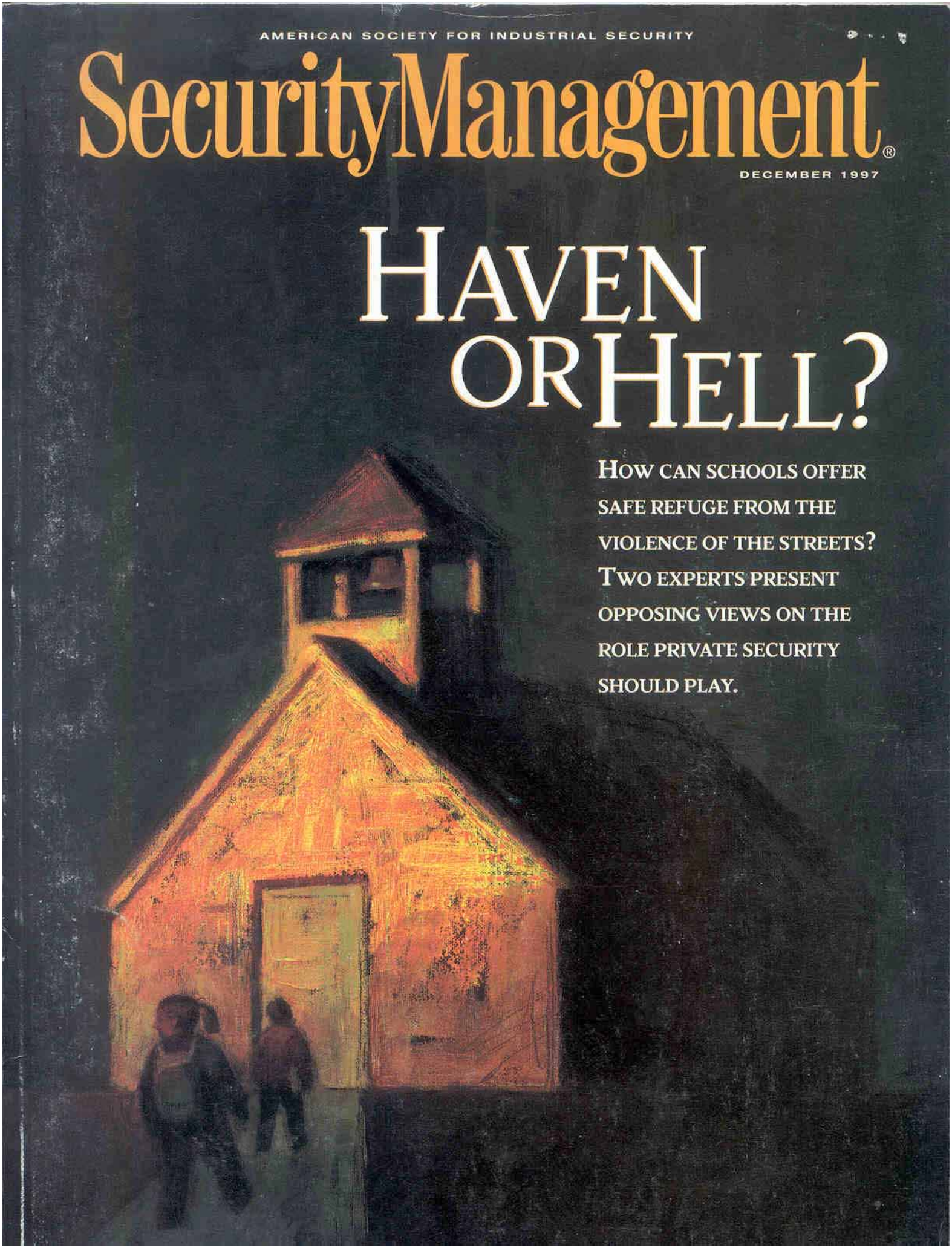
AMERICAN SOCIETY FOR INDUSTRIAL SECURITY

SecurityManagement®

DECEMBER 1997

HAVEN OR HELL?

HOW CAN SCHOOLS OFFER SAFE REFUGE FROM THE VIOLENCE OF THE STREETS? TWO EXPERTS PRESENT OPPOSING VIEWS ON THE ROLE PRIVATE SECURITY SHOULD PLAY.



DEVELOPING A RESPONSE PLAN

BY DOUGLAS A. ROTH

SEARCHING A CORPORATE FACILITY FOR WIRETAPS can be an unnerving experience for all company employees. The very thought that an intruder has been listening to sensitive company discussions can make everyone from the CEO to lower-level supervisors feel violated and mistrustful of coworkers. In addition, because no one knows how much or what type of proprietary information was leaked, serious questions are raised about the company's future ability to compete.

The security professional must be able to put aside these emotions and prepare for the worst. When circumstances require a company to hire a technical surveillance countermeasure (TSCM) team to sweep its offices, the security manager must develop a response plan in the event that a wiretap, bug, or other eavesdropping system is found.

DOCUMENTATION. At a minimum, positive findings should be documented by the TSCM team or security with either still photography, a video camera, or a portable x-ray machine. X-rays are used on the occasions when the illicit devices are discovered hidden inside a wall or pieces of furniture. In other cases, microphones and other devices are in open places such as a light fixture or telephone terminal and can be photographed or videotaped.

The pictures should be presented to senior management to illustrate the problem. They should also be secured as evidence in case charges are brought later.

The TSCM team should generate three copies of these pictures before law enforcement is contacted. The TSCM firm retains one copy and the negatives, the client company is given a copy, and the best copy is provided to law enforcement.

RESPONSE OPTIONS. After the incident has been adequately documented, the company can opt to remove the device, recruit the agent who installed or monitored it, or use the situation to conduct a campaign of misinformation while an investigation is pursued.

Removing devices. Removing the device is the quickest and safest way to end the eavesdropping in the short run. However, unless the perpetrators have been identified and legal action initiated, the company may find that it is under surveillance again in the near future. As a result, most corporations will only remove a bug or wiretap after they determine who installed it.

Recruiting agents. In some cases, corporations intent on gathering information about competitors do not do the work themselves; they hire third-parties to install and monitor listening devices. When these devices are discovered, the security manager and TSCM team may attempt to locate the listening post and recruit the monitoring agent to help in the investigation. This approach works particularly well if the listening agent has been arrested by police for eavesdropping and agrees to cut a deal and identify the party who hired him or her.

Spreading misinformation. Finally, the company may agree to leave the listening device in place and conduct a campaign of misinformation. This tactic might be useful if a company is in the midst of a merger or is negotiating a legal settlement and wants to throw the other party off balance. However, such a strategy should be conducted only under the advice of legal counsel. It is considered risky and may backfire. For example, if misinformation gathered by the spies were leaked to the press, the company could be damaged or forced to take defensive public relations measures.

LEGAL ISSUES. The security manager should be familiar with the basic legal issues that could come up during a TSCM sweep. In general, eavesdropping is considered a criminal violation under federal law. Title 18, Chapter 119 of the U. S. Code prohibits any person from intentionally intercepting—or hiring someone else to intercept—any wire, oral, or electronic communication of another party without that party's knowledge. Most states also have criminal and civil statutes governing illegal wire taps and bugs. The security manager should check with legal counsel to determine which law enforcement jurisdiction to notify.

In the event that a bug is discovered, the security manager and sweep team should treat the area as they would treat any other crime scene. The scene should be cleared, secured, and maintained so as not to disturb any evidence, such as fingerprints, left behind by the person who installed the device. The scene may yield valuable physical evidence when analyzed by a skilled criminal forensics team.

In addition, the security manager and TSCM team may be faced with other legal questions. For example, if the TSCM team has reason to suspect that one of the company's own employees is recording internal meetings where sensitive information is discussed and then passing that information to a competitor, they may want to check the employee's office or desk for tape recorders or other devices. First, however, the security manager should check with corporate counsel to determine whether state law or company policy would consider that activity a violation of the employee's privacy.

Discovering a corporate spy is not the end of a process, but rather the beginning. It is up to the security manager to properly plan a response that comports both with the company's interests and the law. ■

Douglas A. Roth is the president and director of investigations of Investigative Resources International, Long Beach, California.

OTHER RESOURCES

The following is a list of TSCM web sites.

Granite Island Group
James M. Atkinson
http://www.tscm.com

Murray Associates
Kevin D. Murray
http://www.iapsc.org/kmurray

Technical Intelligence Group, Inc.
Steve Wilson
http://www.tscmplus.com

Communication Security, Inc.
Rick Udovich
http://www.bugsweep.com

Ross Engineering, Inc.
Jim Ross
http://www.rosseng.com

Investigative Resources International
Douglas A. Roth
http://www.factfind.com

Future Focus, Inc.
Gordon Mitchell
http://www.pnai.com/pnai_FutureFocus

Electronic Countermeasures, Inc.
William J. Fischer
http://www.t8000.com/eci/eci.htm

Technical Security Consultants, Inc.
Tim Johnson
http://www.amug.org/-dbugman/