

Security CCTV Systems: Risks of Exploitation

by Buzz Benson, EWS, Inc.

Many facilities have Closed Circuit Television Systems to facilitate internal monitoring by key personnel. Cameras are usually placed in areas of high security, at access control points, to monitor foot and vehicular traffic, and to observe special projects and work areas. The goal of security personnel is often to achieve "complete coverage" of the facility by the use of surveillance cameras. Monitoring terminals are generally provided for security stations, executive or command areas, receptionist areas, and within the CCTV system maintenance / distribution area. Distribution cabling is run through non-visible areas to reach appropriate destinations within the facility.

Acquiring recorded video intelligence regarding "areas of high security, controlled access, arrivals and departures, and special projects" may be highly desirable to the criminal eavesdropper or espionage specialist....and that is exactly what a comprehensive CCTV Security System provides. Some systems even provide audio! A criminal eavesdropper may elect to attack these systems and, if successful, monitoring of multiple or individual cameras becomes possible.

Once the desired signals have been acquired, monitoring and recording may take place at the listening post that may be located outside or inside the facility. Acquired signals may be transmitted to the listening post via an installed radio or light transmitter, over power lines, using telephone or LAN cabling, or by another conductive path. The adversary may even use the local cellular system allowing remote dial-up monitoring from anywhere in the world. To complicate detection and isolate the LP, signals may be analog or digital, use many different modulation types, be snuggled or multiplexed alongside other legitimate transmissions, or use a host of other techniques designed to avoid discovery by security personnel.

Remember, the individuals targeting your organization are usually assumed to be outsiders, however they frequently turn out to be assisted by current or past employees, guests, or unescorted service providers with legitimate facility access privileges. Sometimes the adversary is a member the corporate staff!

CCTV systems exploitation can be easily accomplished by the trained operative. Does your facility have a comprehensive CCTV System? Is your CCTV System cabling vulnerable to attack by the criminal eavesdropper? Do access control point cameras allow visual identification of entry codes and procedures? Does the receptionist in your unsecured lobby area have a CCTV monitor?

Security personnel should evaluate their CCTV camera placement and system vulnerability as a part of their on-going TSCM protocol. Points of attack should be secured or eliminated. Considerations should be given not only to technical attacks from the outside...but from the inside as well.

Copyright, all rights reserved, Executive World Services, Inc.

Visit us on the web: <http://www.executiveworldservices.com>